Universidad Carlos III de Madrid

Escuela Politécnica Superior

Ingeniería Técnica en Informática de Gestión

Proyecto Fin de Carrera

Los entornos en nube (Cloud Computing): modalidades, sistemas Cloud en la actualidad, normativa aplicable, controles a considerar y guía de implantación

Autor: Javier Díez Álvaro
Tutor: Miguel Ángel Ramos González

Título: Los entornos en nube (Cloud Computing): modalidades, sistemas Cloud en la actualidad, normativa aplicable, controles a considerar y guía de implantación.
Autor: Javier Díez Álvaro.
Director: Miguel Ángel Ramos González.

EL TRIBUNAL

Presidente:_____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 2 de Octubre de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

"La felicidad solo es verdadera cuando se comparte".

Agradecimientos

En primer lugar quiero agradecer a mis padres, Conchi y Jesús. Por la educación que me han dado, los valores que me han inculcado y por el amor y apoyo que siempre he recibido de ellos. Gracias por todo lo que me habéis dado y me dais cada día.

A mi hermana, Susana, por aguantarme, guiarme y ayudarme siempre. Por ser la persona en la que más confío en todo el mundo, mi mejor amiga. Sin ella no sería lo que soy.

Al resto de mi familia, a mis tíos, a mis primos, por todo lo que me han enseñado y por haber estado no solo en los buenos sino en los malos tiempos. Y a mis abuelos, me acuerdo de vosotros todos los días.

A mis compañeros de la universidad, a mi amiga Patricia, y muy especialmente a mis amigos Jesús, Jaime, Carlos y Álvaro. Habéis sido una de las mejores cosas que me han pasado en estos años. La de cosas que hemos vivido, y las que seguro nos quedan por vivir.

A mi tutor, Miguel Ángel Ramos, por haberme dado la oportunidad de realizar el proyecto fin de carrera con él, y por todas las facilidades que me ha dado a lo largo de este periodo.

Y, por último, a todos los profesores que he tenido en la carrera, porque de todos ellos he aprendido algo.

Resumen

El proyecto trata sobre la computación en la nube, el Cloud Computing, de las diferentes modalidades que hay y de los principales sistemas que existen en la actualidad. Aborda los controles que se han de tener en cuenta a la hora de utilizar estos sistemas e incluye una guía con los pasos que se deben dar para aquellos usuarios que quieran conocer más sobre este tipo de entornos o que se planteen su implantación.

Palabras clave:

Cloud Computing; Entornos en la nube; Computación en la nube.

Abstract

The project deals with the Cloud Computing paradigm, the different existing modes regarding the current systems already implemented. The project addresses the different controls that have to be taken into account when using Cloud Computing systems. It also includes a guide with the steps needed in order to let potential users know more about that kind of environments or the ones that are willing to implement them.

Keywords:

Cloud Computing.

Contenido

1. Introducción y objetivos 17
1.1 Motivación 17
1.2 Objetivos 18
1.3 Estructura de la memoria 19
2. Historia de los entornos en nube 23
2.1 ¿Qué son los entornos en nube? 25
2.2 Antecedentes 28
2.3 El porqué de los entornos en nube 30
3. Tipos de nubes 38
3.1 Private clouds 38
3.2 Public clouds 40
3.3 Hybrid clouds 41
3.4 Community clouds 43
4. Capas 47
4.1 Software as a Service (SaaS) 49
4.2 Platform as a Service (PaaS) 53
4.3 Infrastructure as a Service (IaaS) 54
5. Virtualización 58
5.1 Características 60
5.2 Tipos de virtualización 63
5.3 Sistemas de virtualización 64
5.3.1 Hyper-V 65
5.3.2 VMware 65
5.3.3 XenServer 66
5.3.4 VirtualBox 67
5.3.5 Otros 67
5.4 Papel de la virtualización en Cloud Computing 68
6. Sistemas Cloud Computing utilizados en la actualidad 72
6.1 Empresas de la capa SaaS 72
6.1.1 Salesforce.com 72

6.1.2 Google Apps 75
6.1.3 iCloud (Apple) 78
6.1.4 Microsoft Office 365 80
6.1.5 Zoho 82
6.1.6 Empresas en el mercado español (SaaS) 85
6.2 Empresas de la capa PaaS 91
6.2.1 Google App Engine 91
6.2.2 Force.com y Heroku 96
6.2.2.1 Force.com 97
6.2.2.2 Heroku 99
6.2.3 Windows Azure Platform 101
6.2.4 Empresas en el mercado español (PaaS) 103
6.3 Empresas de la capa IaaS 105
6.3.1 Amazon Web Services 106
6.3.1.1 Servicios de Procesamiento de datos. 106
6.3.1.2 Servicios de Almacenamiento de datos 108
6.3.1.3 Servicios de Redes 110
6.3.1.4 Servicios de Entrega de contenido 111
6.3.1.5 Servicios de Bases de Datos 112
6.3.1.6 Servicios de Mensajería 113
6.3.1.7 Servicios de Pagos y facturación 114
6.3.1.8 Servicios de Despliegue y gestión 115
6.3.1.9 Servicios de Soporte 116
6.3.1.10 Servicios de Tráfico Web y Personal 116
6.3.2 GoGrid 117
6.3.3 Empresas en el mercado español (IaaS) 120
7. Control en Cloud Computing 131
7.1 Legislación 131
7.1.1 Regulación de la LOPD 133
7.1.2 Regulación de la LSSI 169
7.1.3 Regulación del Código penal 171
7.2 Riesgos de la utilización de entornos en nube 174
7.2.1 Riesgos de Infraestructura 174
7.2.1.1 Abuso y mala utilización del Cloud Computing 174
7.2.1.2 Amenaza interna 176
7.2.1.3 Pérdida de información importante 177
7.2.1.4 APIs e Interfaces inseguras 178

7.2.1.5 Suplantación de identidad 180
7.2.1.6 Problemas derivados del Hardware compartido 181
7.2.1.7 Planes inadecuados frente a desastres 182
7.2.1.8 Desconocimiento del perfil de riesgo 183
7.2.2 Riesgos técnicos 185
7.2.2.1 Compartición de recursos 185
7.2.2.2 Abuso de privilegios 186
7.2.2.3 Dimensionamiento inadecuado de recursos asignados 187
7.2.2.4 Comunicaciones inseguras entre cliente y proveedor 188
7.2.2.5 Eliminación de la información 188
7.2.2.6 Denegación de servicio 189
7.2.2.7 Insolvencia del proveedor Cloud 190
7.2.3 Riesgos legales y contractuales. 191
7.2.3.1 Deslocalización de la información 191
7.2.3.2 Protección de datos 192
7.2.3.3 Dependencia del proveedor 192
7.2.3.4 Titularidad de los derechos 193
7.2.3.5 Notificación frente a incidentes graves de seguridad 193
7.2.3.6 No disponibilidad del servicio por parte del proveedor 194
7.2.3.7 Incumplimiento de algún otro tipo de directrices 195
8. Guía de migración a la nube 198
8.1 Análisis de la situación de cliente 198
8.2 Análisis DAFO 202
8.3 Análisis de la elección del modelo en la nube 204
8.4 Análisis de los proveedores Cloud existentes 205
8.5 El contrato 206
8.6 Cómo realizar la migración a la nube 209
9. Planificación y presupuesto 213
9.1 Planificación inicial 213
9.2 Planificación final 215
9.3 Presupuesto 217
10. Conclusiones 220
11. Referencias y bibliografía 223
11.1 Referencias 223
11.2 Bibliografía 227

Índice de Ilustraciones

Ilustración 1 - Tipos de Nubes [3] 43
Ilustración 2 - Community Cloud [4] 44
Ilustración 3 - Capas [5] 48
Ilustración 4 – Virtualización [6] 58
Ilustración 5 - Virtualización 2 [7] 60
Ilustración 6 - Hyper-V [8] 65
Ilustración 7 – Vmware [9] 65
Ilustración 8 - Xen Server [10] 66
Ilustración 9 – VirtualBox [11] 67
Ilustración 10 – Salesforce [12] 72
Ilustración 11 - Google Apps [13] 75
Ilustración 12 - Google Apps 2 [14] 77
Ilustración 13 – iCloud [15] 78
Ilustración 14 - Office 365 [16] 80
Ilustración 15 – Zoho [17] 82
Ilustración 16 - Google App Engine [18] 92
Ilustración 17 - Force.com & Heroku [19] 97
Ilustración 18 - Force.com [20] 97
Ilustración 19 – Heroku [21] 99
Ilustración 20 - Windows Azure [22] 101
Ilustración 21 - Amazon Web Services [23] 106
Ilustración 22 – GoGrid [24] 117
Ilustración 23 - Planificación inicial 214
Ilustración 24 - Planificación final 216

Índice de Tablas

Tabla 1 - Software as a Service 52
Tabla 2 - Riesgos Cloud Computing 196
Tabla 3 - DAFO 204
Tabla 4 - Presupuesto 218

Capítulo 1:

Introducción y objetivos

1.Introducción y objetivos

En este primer capítulo se explica la motivación de este proyecto fin de carrera, sus objetivos y una descripción de cada uno de los capítulos que componen este documento.

1.1 Motivación

Este proyecto trata sobre el Cloud Computing o también llamado computación en la nube. Como se explicará a lo largo de este documento, este nuevo sistema ofrece una serie de servicios bajo el pago por uso a través de Internet, con lo que la idea del uso de software o hardware cambia con respecto a lo que se hacía hasta ahora.

El tema del Cloud Computing es un tema muy importante, ya que muchas empresas están trasladando sus servicios a la nube en los últimos tiempos. Según ha publicado TICbeat en el mes de julio de 2012, 8 de cada 10 empresas ya utilizan algún tipo de solución Cloud [1], y como dice, estas cifras podrían aumentar teniendo en cuenta las previsiones de inversión.

De la misma manera, la misma empresa TICbeat publicó en el mes de marzo de 2012 que más del 60% de las empresas españolas que tienen conexión a Internet utilizan algún tipo de solución en la nube, lo que supone un crecimiento con respecto al año 2011 [2].

Viendo estos resultados del estudio realizado por TICbeat, podemos deducir la importancia que están ganando los entornos en nube día a día.

Los problemas que se pretenden resolver son varios: que el público, usuarios, empresas, etc. se familiaricen con este nuevo modelo, que sepan en qué se basa, qué características tiene, los servicios que puede ofrecer, dar a conocer los proveedores de servicio que existen en la actualidad, los controles que se han de tener en cuenta a la hora de utilizar este tipo de servicios, y, en el caso de que al final quieran dar el salto a la nube, una guía de los pasos que se deben realizar para esto sea posible.

Este documento dará respuesta a todos estos problemas y más.

1.2 Objetivos

Los objetivos que se persiguen cumplir en este proyecto fin de carrera son los siguientes:

- Objetivo 1: Definir de forma clara qué es el Cloud Computing, ya que hay mucha gente que sabe que existe, pero muy pocas personas saben qué es y en qué consiste realmente. Asimismo, ver por qué surgió este nuevo modelo cuando ya existía uno que satisfacía esas necesidades, además de ver las ventajas que tiene la computación en la nube con respecto a lo que ya había antes.

- Objetivo 2: Saber clasificar y tener claro los tipos de nubes que existen y los servicios que puede ofrecer dentro de las distintas capas que existen en Cloud Computing.

- Objetivo 3: Aclarar el papel de la virtualización en la computación en la nube. Hay mucha gente que no tiene claro este concepto, además de algunos confunden ambos términos.

- Objetivo 4: Dar a conocer un amplio abanico de sistemas Cloud existentes hoy en día, con especial atención y enfoque a los presentes en territorio Español.

- Objetivo 5: Aclarar y facilitar la legislación aplicable a los entornos en nube, ya que no existe ningún marco que regule este nuevo sistema ni en nuestro país ni a nivel global.

- Objetivo 6: Proporcionar una serie de pasos que se han de seguir para aquellas personas, usuarios u organizaciones que quieran implantar la nube.

- Objetivo 7: En conclusión, dar a conocer este nuevo modelo a todo el mundo, ya que tiene un gran futuro en el mundo de las tecnologías de la información y la comunicación.

1.3 Estructura de la memoria

Este documento está organizado siguiente la siguiente estructura:

- Capítulo 1: Introducción y objetivos – Se explica

- Capítulo 2: Historia de los entornos en nube – En este capítulo se explica qué son los entornos en nube y en qué consiste este sistema. También se habla de los antecedentes que había antes del nacimiento de este nuevo modelo, y el porqué del nacimiento del Cloud Computing, qué beneficios puede aportar con respecto a lo que ya existía previamente.

- Capítulo 3: Tipos de nubes – En esta sección se describen todos los tipos de nubes que existen en Cloud Computing así como sus características y diferencias entre ellas.

- Capítulo 4: Capas - En este capítulo se definen las capas de servicio con las que cuentan los entornos en la nube. Dependiendo del servicio que se quiera contratar, estos servicios pertenecerán a una u otra capa del Cloud Computing.

- Capítulo 5: Virtualización – Se define el significado de virtualización, así como su relación e implicación en la computación en la nube. Se describen las diferentes características que tiene, los tipos de virtualización que existen, y se ponen algunos ejemplos de sistemas de virtualización que hay.

- Capítulo 6: Sistemas Cloud Computing utilizados en la actualidad – En esta sección vamos a ver importantes ejemplos de sistemas Cloud utilizados hoy en día, prestando especial atención a los que se ofrecen en territorio español. Estas empresas que ofrecen servicios en la nube están clasificadas según las tres capas que hemos visto en el capítulo 4.

- Capítulo 7: Control en Cloud Computing – En este capítulo se trata la legislación aplicable a los entornos en la nube desde tres puntos de vista:

la regulación de la LOPD, la regulación de la LSSI y la regulación del Código penal. Además, de describen los principales riesgos que existen al utilizar los servicios Cloud Computing.

- Capítulo 8: Guía de migración a la nube – Se describen los pasos que se deben ir dando si una persona física o entidad quiere dar el salto a la nube.

- Capítulo 9: Planificación y presupuesto - En esta sección se describe, por una parte la planificación realizada para llevar a cabo este proyecto fin de carrera, y por otro lado el presupuesto necesario para llevarlo a cabo.

- Capítulo 10: Conclusiones – En esta sección se analizan las conclusiones finales que se sacan después de haber realizado este proyecto.

- Capítulo 11: Referencias y bibliografía – En este último capítulo del proyecto se recoge todo el material consultado para la buena realización de este proyecto.

Capítulo 2:

Historia de los entornos en nube

2.Historia de los entornos en nube

El término "nube" se utiliza como metáfora de Internet, para reproducir su infraestructura, ya utilizada en el pasado para representar la red de telefonía. Más adelante se empezó a utilizar para simbolizar Internet en los diagramas de redes informáticas como abstracción de la infraestructura que representa.

Las referencias históricas en orden cronológico de este tema son las siguientes:

- La primera vez que se usó el concepto *computación en nube* fue en los años 60, cuando John McCarthy, (un importante informático nacido en EEUU (1927-2011) que entre otras cosas tuvo importantes contribuciones en el campo de la Inteligencia Artificial), dijo que "algún día la computación debería organizarse como un servicio público".

- Douglas Parkhill, (Tecnólogo nacido en Canadá y ex ministro de investigación, conocido por su trabajo pionero en el cómputo en nube), en su libro publicado en 1966 "*The Challenge of the Computer Utility*", investigó minuciosamente conceptos tales como la mayoría de características actuales del Cloud Computing (previsión elástica, siempre online, producto como servicio, etc.).

- En 1990 el término *nube* fue robado por la telefonía con las redes privadas virtuales (denominadas VPN). Esto es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada (por ejemplo, la posibilidad de conectar dos o más sucursales de una empresa utilizando un vínculo de Internet, permitir a los trabajadores la conexión desde su casa al centro en sí, etc.).

- En 2006, la empresa Amazon dio un paso importante cuando actualizó sus centros de datos. Decir que entonces las redes de ordenadores solo utilizaban un 10% de su capacidad.

- En 2007, las empresas Google e IBM, y una serie de universidades comenzaron un gran proyecto de investigación sobre la computación en nube. Este hecho coincidió en el tiempo con la ganancia de popularidad de este término por parte de la prensa.
  Para mediados de 2008 ya había numerosos eventos sobre el Cloud Computing.

- En 2008, Garnet (una empresa estadounidense que realiza investigación y análisis para las industrias de hardware computacional, software, comunicaciones y de tecnologías de la información TI) observó que las empresas estaban empezando a cambiar el modelo de propiedad de software-hardware por el modelo basado en el uso por servicio. Además, también previó que ese cambio hacia la *nube* se traduciría en un crecimiento masivo en productos TI en ciertas áreas y en una reducción en otras.

- También en ese 2008, Eucalyptus (una infraestructura *open source* para la implementación de computación en nube privada) se convirtió en el primer código abierto compatible con el API de "Amazon Web Services" (AWS) de la plataforma para el despliegue de nubes privadas.

- Por último, en 2010 Microsoft declaró que sobre el 75% de su gente estaba haciendo todo o inspirado o completamente en la *nube*, y que dentro de un año llegaría al 90%.

A continuación vamos a definir qué son el Cloud Computing, sus antecedentes y el porqué del nacimiento de esta nueva tecnología.

2.1 ¿Qué son los entornos en nube?

También conocido como Cloud Computing, procesos en nube o nube de conceptos, es un sistema que permite ofrecer una serie de servicios a través de Internet. Todo lo que se ofrece, se ofrece como servicio.

Esto tiene su punto positivo en que los usuarios pueden acceder a los distintos servicios disponibles en Internet sin llegar a tener un conocimiento de lo que hay detrás, como la gestión de recursos que se usan para mover esas aplicaciones, por ejemplo.

Se trata de un paradigma en el que la información se almacena de manera permanente en servidores de Internet, y se envía a cachés temporales de los clientes (los datos de los usuarios, el software como servicio, no estarán en nuestros equipos ni dependerán de las limitaciones que puedan tener estos). Por ejemplo, todos los archivos, información, datos, etc. que tenga y/o maneje un usuario concreto, permanecerán en Internet, en la "nube", de manera que no tendremos que preocuparnos de si tenemos el espacio suficiente en nuestro equipo para almacenar todo ese conjunto de información. En definitiva, toda la información, procesos que se estén ejecutando, datos, etc. se localizan en Internet (en servidores), por lo que todo el mundo puede acceder a la información completa, sin la necesidad de tener una gran infraestructura personal, y desde cualquier sitio que disponga de una conexión a Internet.

Uno de los principales cambios que ofrece con respecto a lo que hay hasta ahora, es que permite aumentar los servicios basados en la red. Al final, esto genera beneficios tanto a los proveedores como a los usuarios. A los proveedores porque pueden ofrecer una mayor cantidad de servicios y de forma más rápida, y a los usuarios porque podrán acceder a ese mayor catálogo de servicios, de forma rápida y transparente.

En este punto podemos introducir una de las características más importantes de la computación en nube, *el consumo bajo demanda*: Se tendrán un conjunto de servicios que el usuario tendrá a su disposición, y, en caso de tener un pico de demanda no previsto (un momento en el que se necesite realizar una mayor cantidad de trabajo en el mismo tiempo, por ejemplo), se le podrá aprovisionar al instante, pagando solamente por el consumo que se haya efectuado. Esto es lo que se denomina un modelo de pago por consumo. Lo que conocíamos hasta ahora era el pago por una licencia de un producto para poder utilizarlo completamente.

Otra de las principales características del Cloud Computing es que incorpora el concepto Software como servicio (que viene del inglés SaaS: Software as a Service, y que se define como modelo de distribución de software donde tanto el software como los datos que se utilizan se guardan en servidores de Internet). Esto es que, al tratarse de un modelo en que se distribuye software, tanto el software como los datos que se manejan se almacenan en servidores. El proveedor se encarga del mantenimiento, operación diaria y soporte del software usado por el cliente. De esta forma, el ahorro en tiempo, dinero, etc. con respecto al modelo que se ha utilizado hasta el momento puede llegar a ser muy alto.

La lista completa de principales características de la computación en nube son las siguientes:

- Autoservicio de servicios bajo demanda: El usuario tiene acceso a la serie de aplicaciones, recursos, etc. disponibles en la *nube*, sin necesidad de tener ningún tipo de interacción ni negociación con el proveedor, con la posibilidad de aumentar o disminuir el volumen de recursos según lo que necesite en cada momento.

- Accesibilidad: Los servicios, al estar emplazados en la nube, son accesibles desde cualquier terminal con acceso a Internet, ya sean ordenadores, tablets, PDAs, smartphones, etc.

- Fondo común de recursos: Los servicios están disponibles en la nube, para que la globalidad de los usuarios tengan acceso a ellos. A su vez, los recursos están en reservas en común para que sean asignados a los usuarios según su necesidad, y pueden estar ubicados por centro de datos, por provincia, por país, etc. Así, los recursos son asignados y reasignados conforme a la demanda del consumidor en cada momento.

- Elasticidad y escalabilidad: La cantidad de servicios y recursos se puede aumentar o disminuir según las necesidades del usuario o cliente en cada momento. En ciertos casos se puede hacer de forma automatizada en función de la demanda. Desde el punto de vista del cliente, la capacidad es ilimitada y se puede acceder a cualquier cantidad de servicios y recursos en cualquier momento.

- Servicio medido: Al tener los servicios, recursos, etc. en la nube, es necesario que cada uno de ellos sea medido en cada momento, para

poder llevar a cabo un control de la utilización de cada uno. Así, se evitará un posible colapso de algún servicio o recurso. Además, en caso de que algún servicio sea de pago, esa medición se realizará para su posterior tarificación.

2.2 Antecedentes

Antes del nacimiento de la computación en nube, siempre hemos tenido que instalar el software en el equipo en que queramos utilizarlo. Por ejemplo, si alguien quería utilizar un programa de edición de video, se compraba el CD de instalación, lo instalaba, lo configuraba, etc. y ya podía utilizarlo. En el supuesto de que el usuario necesitara que una persona que está al otro lado del planeta pudiera ver el trabajo que ha estado haciendo, y continuar con él, entonces necesitaría otro CD de instalación, otra licencia…

Además de todo esto, la cantidad de hardware y software necesario para poder ejecutar las aplicaciones en cada uno de los equipos en que se requiriera sería bastante alta, con el gasto asociado que ello conlleva.

En definitiva, aparte del software que se necesitaba, había que tener en cuenta aspectos tales como: el número de licencias, su mantenimiento, el crecimiento en hardware y en espacios físicos que generaría el tener nuevo software, así como el aumento de recursos humanos.

Otro punto de vista a tener en cuenta son las tecnologías a las que tenemos acceso actualmente, cosa que no pasaba hace unos años:

Actualmente, es normal que una persona tenga un ordenador personal en casa (si no varios), otro en la oficina, un smartphone (Iphone, HTC, Samsung Galaxy…), además de poder acceder a ordenadores públicos en cualquier lugar (ya sea en un hotel, una biblioteca, un cibercafé, etc.). Esto crea un problema de sincronización en las aplicaciones que pueda usar una persona, ya que puede tener diferentes datos o fechas de modificación en cada uno de los dispositivos que puede usar a lo largo de una jornada.

Si tuviéramos este escenario cuando no existía el Cloud Computing, no podríamos hacer uso de todos los dispositivos con los que contamos, y si quisiéramos poder usar todos, tendríamos que tener una licencia del software que queremos usar por cada dispositivo en el cual quisiéramos utilizarlo. Tendríamos que guardar una versión de nuestro trabajo cada vez que hiciéramos cambios, y llevárnosla a los restantes dispositivos, para que cuando continuáramos el trabajo en cualquiera de ellos, partiéramos de la última modificación realizada…

Como podemos ver, esto sería prácticamente inviable. Y es aquí donde la Computación en nube nos soluciona todos estos problemas, ya que nos otorga una flexibilidad de la que hasta ahora no disponíamos.

Llegados a este punto, la pregunta que nos podemos hacer es si estamos preparados para usar la nube. ¿Lo estamos?

Esta es una pregunta muy importante a la que tenemos que dar respuesta. En los últimos años ha habido una masificación de los ordenadores, un crecimiento exponencial de Internet así como un crecimiento abrumador del ancho de banda de Internet. Todo esto favorece el que podamos plantearnos el salto a esta nueva tecnología. Además, el impacto cultural que ha tenido Internet en la

última década es muy significativo. Por todo esto, podemos dar una primera impresión sobre esta cuestión, favorable al cambio a la Computación en nube.

2.3 El porqué de los entornos en nube

En puntos anteriores hemos definido qué son los Entornos en nube, se han dado una serie de datos históricos, y se ha hablado de cómo funcionaban las cosas antes de la aparición de esta nueva tecnología.

El Cloud Computing está pensado tanto para el ámbito personal como para el ámbito empresarial. Para el ámbito personal (para el usuario final) ya existen varias aplicaciones que usan esta tecnología. En cambio, para el sector que se ve que se puede tener un gran crecimiento es para el sector empresarial.

Para explicar esto, vamos a plantear un ejemplo de un negocio cualquiera hasta la aparición del Cloud Computing, y los cambios que habría si se pasaran a la nube:

Hasta ahora, en el mundo empresarial se necesitan aplicaciones que tienen un alto coste por las licencias, el mantenimiento, etc. Véase:

- La licencia de un producto software se paga siempre, aunque solo se vaya a usar una parte del total del software que estamos pagando.

- Por otro lado, está demostrado que el mantenimiento del software puede llegar a ser la parte más costosa del ciclo de vida de un producto (entre el 60 y el 90% del coste total). El coste de este mantenimiento puede llegar a

ser tan alto como perder oportunidades de nuevos desarrollos por falta de tiempo, posibles perjuicios en otros desarrollos que se estén llevando a cabo cuando la plantilla tiene que dejarlos, parcial o totalmente, para atender peticiones de mantenimiento de otro software, etc.

A todo esto, tenemos que unir todo lo que hay detrás de cualquier negocio o empresa: oficinas, centro de datos, alimentación, ancho de banda, redes, servidores, almacenamiento, etc. para poder ejecutar y mantener ese software que pagamos. Como es lógico, también se necesita un personal preparado que se encargue de la instalación, configuración, y del mantenimiento comentado. Además de todo esto, son necesarios entornos de desarrollo, preproducción, producción. Y todo esto lo hacen las empresas para poder tener competitividad con otras empresas.

Con la computación en nube todo este escenario cambia. Para empezar, no se ejecutarían las distintas aplicaciones en local, sino en un sitio compartido (Internet). Esto quiere decir que todo lo que necesitamos hasta ahora para poder utilizar estas aplicaciones empresariales ya no nos haría falta. Poniendo un ejemplo, podríamos fijarnos en GMAIL, para el que no necesitamos ni servidores de almacenamiento, ni tener nada instalado, etc.

Aquí es donde cambia el concepto del Software. Como sabemos, hasta ahora se tenía que pagar la licencia del software, tenerlo instalado y configurado. Ahora solo tendríamos que acceder a la aplicación desde la Web. Como hemos mencionado anteriormente, se prevé un crecimiento muy grande en el entorno empresarial, puesto que las ganancias pueden llegar a ser bastante significativas con respecto a lo que se tenía hasta ahora.

Las ventajas más importantes del Cloud Computing son las siguientes:

- Se reducirán costes tanto operativos como administrativos. Algunos de estos son:

    - Se puede llegar a tener un coste nulo en la inversión inicial de infraestructura, ya que la mayoría de esta la proporcionará el proveedor de la nube (servidores, routers, personal capacitado para su operación, etc.).
      Por esta razón, el riesgo que una empresa toma a la hora de comenzar un nuevo proyecto será menor.

    - Las licencias del software.

    - El mantenimiento del software (que como dijimos con anterioridad, puede llegar a ser la parte más costosa del ciclo de vida de un software).

    - El personal encargado de la instalación y configuración del software.

    - El hardware necesario para que el software se ejecute de forma eficiente en cada uno de los equipos donde se tenga que usar.

- Infraestructura "justo a tiempo": Un problema típico de una empresa a la hora de comenzar cualquier proyecto es prever el dimensionamiento que tendrá, lo que deriva en una inversión en recursos, personal, etc. Más tarde, si ese proyecto tuviese un éxito mayor del esperado inicialmente, el hacer una reinversión para poder tener más recursos es un gran problema. Por otro lado, puede pasar que el éxito del proyecto no llegue

a lo esperado, por lo que se habría invertido más de lo necesario en el proyecto en cuestión.

Todos estos problemas son resueltos con el modelo de computación en la nube ya que en cada momento se podrá aumentar o disminuir los recursos que se necesitan.

- Aumentará la *flexibilidad*: Completando el punto anterior, al pasar a un modelo de pago por consumo, se podrá satisfacer un pico de demanda de cierta aplicación, de recursos, etc. de forma rápida y sencilla.

- La forma de pago cambiará: Al terminar con las licencias, se pagará por lo que se usa, es decir, será un pago por uso. Dicho de otra forma, se hará un "alquiler" de la aplicación. Así, se pagará por lo que realmente se utiliza, en lugar de pagar por toda una aplicación cuando a lo mejor luego solo se utiliza una pequeña parte (como ocurría antes con las licencias).

- Se ganará en *movilidad* y *sincronismo*: Tendremos acceso a la información y podremos realizar nuestro trabajo (o a cualquier cosa que tengamos en la nube) debido a que se podrá acceder a la nube desde cualquier dispositivo que tenga acceso a Internet. Además, como todo lo que realicemos se guardará en Internet, en la nube, cuando accedamos de nuevo, tendremos lo último que hayamos hecho la última vez que accedimos y modificamos algo (como si estuviéramos en nuestro ordenador personal, que lo apagamos, y cuando iniciamos de nuevo, tenemos toda la información disponible).

- En el caso de que haya alguna actualización en los servicios, alguna corrección en algún servicio que no funciona correctamente o alguna

nueva funcionalidad, estos cambios se harán automáticamente, por lo que el cliente tendrá acceso inmediato a dichas mejoras.

- Desde el punto de vista ecológico, si cada empresa dejara de tener su propio centro de datos, se ahorraría mucha energía, lo que cada vez es más importante en la sociedad.

Todo esto permitiría a la empresa en cuestión centrarse en el negocio específico al que se dedica, en lugar de desviar gran cantidad de recursos poder llevar a cabo ese trabajo. Un ejemplo concreto sería para las pequeñas empresas, que podrían competir con mayor igualdad de condiciones desde el primer día.

Aunque el ejemplo anterior es para una empresa cualquiera, los beneficios que puede llegar a tener un usuario particular con respecto a las condiciones que tuviera antes de la llegada de la Nube también son altísimos.

En cambio, hay una serie de aspectos que pueden llegar a generar reticencias en el cliente final (tanto para el sector empresarial como para un usuario particular).

Las principales desventajas de la computación en nube son las siguientes:

- Los datos, al estar en la nube, estarían en manos de terceros. Esto puede generar intranquilidad por parte de los usuarios, al no tener su información ellos mismos. Por esto mismo, el proveedor ha de ser de total confianza, con el fin de que le asegure puntos como la confidencialidad de los datos que manejan y guardan.

Así, la privacidad es uno de los puntos que más pegas o problemas puede dar a la hora de pasarse a la computación en nube.

- El hecho de que los datos se encuentren en Internet, hace que el nivel de seguridad de los entornos en nube pase a tener un papel protagonista, puesto que todo el trabajo, datos, información de una empresa, usuario, etc. estarán depositados en la nube (este apartado se verá con mucha más profundidad más adelante). También, el poder acceder a los datos en cualquier momento, independientemente del sitio en el que se esté, debe estar asegurado para los clientes.

- Continuando con el tema de la seguridad de los datos, un punto crítico es dónde se guardan los datos personales de los usuarios. Como no sabemos dónde se encuentran los datos en ningún momento, puede ocurrir que los datos personales se estén guardando en un país con un nivel de protección de datos no adecuado a la clasificación hecha por la Agencia Española de Protección de Datos (que en su Web www.agpd.es enumera los países que cumplen el nivel de protección de datos del Espacio Económico Europeo y que veremos más adelante).

- La dependencia de Internet para poder acceder a los servicios, software, información, datos, etc. En definitiva, se depende de una buena conexión y fiable a Internet. Porque si nos quedamos sin Internet, no se podría hacer nada.

  Asimismo, si los proveedores del servicio tienen que hacer alguna interrupción para realizar labores de mantenimiento, los usuarios no podrían realizar ninguna operación hasta que terminasen esos trabajos por parte del proveedor.

- Recuperación: El hecho de desconocer la localización de la información y los datos por parte de los usuarios o propietarios, no ha de interferir en ningún momento con la labor esencial de recuperación de la información por parte del proveedor en caso de desastre o pérdida de estos.

- Relación perpetua: Esto es, que la sostenibilidad del proveedor ha de estar asegurada. Eventos como cambios en el negocio del proveedor, fusiones, etc. no pueden dejar desamparado al cliente, por lo que se debería firmar un compromiso de continuidad a largo plazo en la relación existente entre proveedor y cliente.

- Servicios del catálogo poco personalizables: Los proveedores ofrecerán un catálogo de servicios al usuario final. El problema es que estos servicios serán, por lo general, iguales para todos, por lo que si una empresa en concreto necesita una modificación específica de uno de los servicios que ofrece el proveedor, será difícil satisfacer las necesidades de esa empresa.

Teniendo en cuenta todas les desventajas mencionadas anteriormente, cabe resaltar que tanto la privacidad de los datos como la seguridad de los mismos son los puntos más críticos. Y es así porque aparte de lo mencionado con anterioridad, existe un riesgo de que los datos e información sean interceptados o modificados por terceras personas mientras están "viajando" de un sitio a otro (ya que se almacena en la nube y luego los usuarios usan esa información).

Capítulo 3:

Tipos de nubes

3.Tipos de nubes

En Cloud Computing existen distintos tipos de nubes. Dependiendo de las necesidades que se tengan y la finalidad que se busque, se elegirá un tipo de nube u otro. Cada uno de los cuatro tipos que hay tiene un fin para el que fueron creadas, así como una serie de características concretas. En cambio, hay una serie de aspectos donde los cuatro tipos de nubes coinciden, y son en la seguridad, en la gestión del hardware que se utiliza y en las aplicaciones que se requieren.

A continuación pasamos a definir cada tipo de nube que hay.

3.1 Private clouds

Este tipo de nubes ofrecen un mayor nivel de seguridad y control en los datos e información que se manejan. Normalmente las nubes privadas suelen encontrarse dentro de las instalaciones del usuario o de la empresa a la que pertenezca estando dentro del país donde esté la propia organización, y es la propia entidad la que decide que procesos se ejecutan, dónde se ejecutan y quién puede ejecutarlos. Así, el conjunto de servicios e infraestructura que proporciona se alojan en una red privada, y habitualmente no suelen ofrecer servicios a terceros.

Una de las ventajas que tienen las nubes privadas es la localización de los datos. Puesto que el Cloud se encuentra dentro de las instalaciones de la organización o del usuario final, se tiene una mayor seguridad de los datos, aparte de que

sabemos en todo momento dónde están localizados. Además, en una empresa será más fácil integrar el resto de servicios y equipos que se tienen con la nube privada.

En cambio, hay una desventaja directamente ligada con las ventajas que hemos descrito. Al tener la nube dentro de las instalaciones de la propia entidad, se tendrá que hacer una inversión inicial en infraestructura (equipos, servidores, etc.), sistemas de virtualización, seguridad y control, ancho de banda, etc. sin olvidar el gasto de mantenimiento que conlleva. Por esta razón, el retorno de la inversión inicial será un proceso más lento que si eligiéramos una nube pública en lugar de este tipo de nube. Además, una repercusión de la inversión inicial que se necesita es la pérdida de escalabilidad que se tiene con otro tipo de nubes.

Por todo ello, y teniendo en cuenta las ventajas e inconvenientes de este tipo de nubes, es idóneo para aquellas organizaciones y entidades que necesiten una alta protección y control de los datos que se manejan, de los procesos que se ejecutan y de las ediciones a nivel de servicio que se tienen como puede ocurrir en algunos casos de las administraciones públicas. Cabe decir que habitualmente las nubes privadas se utilizan para la obtención de máquinas, almacenamiento, infraestructura de red, es decir, para servicios de la capa Infraestructura como Servicio (IaaS), pero también es posible tener nubes privadas en las que se puedan implementar y desplegar aplicaciones (servicios de la capa PaaS) y que ofrezcan servicios finales (como en la capa SaaS).

3.2 Public clouds

Las nubes públicas tienen la principal diferencia con respecto a las nubes privadas en que los servicios que se ofrecen se encuentran en servidores externos al usuario u organización, no como en las nubes privadas que se encontraban en las mismas instalaciones de la empresa. El acceso a estos servicios se puede hacer de forma gratuita o mediante el pago de un alquiler por uso (dependiendo de la empresa proveedora de la nube pública).

De esta manera, la información, los datos o los trabajos de un cliente de la nube pública pueden estar dispersos y mezclados con información de otros usuarios entre los distintos servidores, sistemas de almacenamiento u otras infraestructuras de la nube pública.

Una de las ventajas más importantes de la utilización de nubes públicas es la alta capacidad de procesamiento y almacenamiento sin la necesidad de instalar nada en nuestra máquina local, y sin tener que realizar una inversión inicial ni ningún gasto de mantenimiento, pagando solo por lo que se use en cada momento o abonando una suscripción por utilización. Así, el retorno de la inversión se realiza de forma más rápida en este tipo de nubes, y más si lo comparamos con las nubes privadas.

Una de las principales desventajas de usar este tipo de nubes es que, al dejar el mantenimiento, la carga operacional, la seguridad y la gestión de nuestros datos e información en manos de terceros (proveedor del hardware y software de la nube pública), no sabremos en ningún momento dónde se encuentran nuestros datos (en contraposición con la nube privada, que en todo momento sabemos dónde está la información y los datos que maneja la compañía). Además, al igual que los datos de una empresa, la información de muchas otras

(miles o millones) entidades estarán en la nube, pudiendo compartir servidores, sistemas de almacenamiento, etc. por lo que la seguridad puede llegar también a ser un problema.

Otro problema es la dependencia de tener los servicios que ofrece el proveedor de la nube siempre en línea, ya que si en un momento dado un cliente no pudiera acceder a las aplicaciones, datos o información que están en la nube, sería un problema muy grave. Además, al ser un servicio totalmente externo al usuario final o a la organización en cuestión, puede llegar a ser muy costoso el integrar el resto de servicios de la entidad con los servicios de la nube.

3.3 Hybrid clouds

Este tipo de nubes combinan los dos tipos de nubes vistos anteriormente: las nubes privadas y las nubes públicas, cogiendo lo mejor de cada una de ellas. Así, en las nubes híbridas, el cliente será propietario de algunas partes (nube privada) y compartirá otras (nube pública), pero siempre manteniendo un control de toda la estructura.

De esta manera, las empresas pueden controlar sus principales aplicaciones que realizan los procesos más críticos a la vez que aprovechan el Cloud Computing de la nube pública en los lugares donde les convenga.

Este tipo de nube tiene una ventaja que viene de combinar las nubes públicas y privadas. Requiere una inversión inicial menor que la que se requiere para las nubes privadas, y además tiene la posibilidad de tener los servicios de las capas

Software as a Service, Platfortm as a Service e Infrastructure as a Service bajo demanda, como en la nube pública.

Así, en un momento de necesidad, se puede escalar la plataforma todo lo que se necesite sin la necesidad de invertir nuevamente en infraestructura. Luego, si a lo largo del tiempo se ve que esta necesidad se vuelve algo estable, se podría incrementar la capacidad de la nube privada así como pasar algunos de los servicios que se necesiten y que estén en la nube pública a la nube privada. Por otra parte, si resulta que esas necesidades de escalabilidad son algo puntual, se podría continuar igual sin ampliar la infraestructura privada de forma innecesaria.

Uno de los problemas de este tipo de nubes es la complejidad que existe a la hora de determinar la distribución de las aplicaciones a través de estos dos ambientes contrapuestos, es decir, cómo distribuir las aplicaciones entre la parte pública y la parte privada de la nube híbrida. Otro problema que se desprende de este tipo de nubes es saber si todos los aspectos del negocio de la entidad se podrán comunicar entre sí.

A continuación podemos observar una figura donde se aprecian los tres tipos de nubes descritos hasta el momento, y la relación que guardan unas con otras. Por ejemplo, se ve como la nube híbrida tiene parte de nube privada y parte de nube pública, mientras que estas dos no se relacionan.

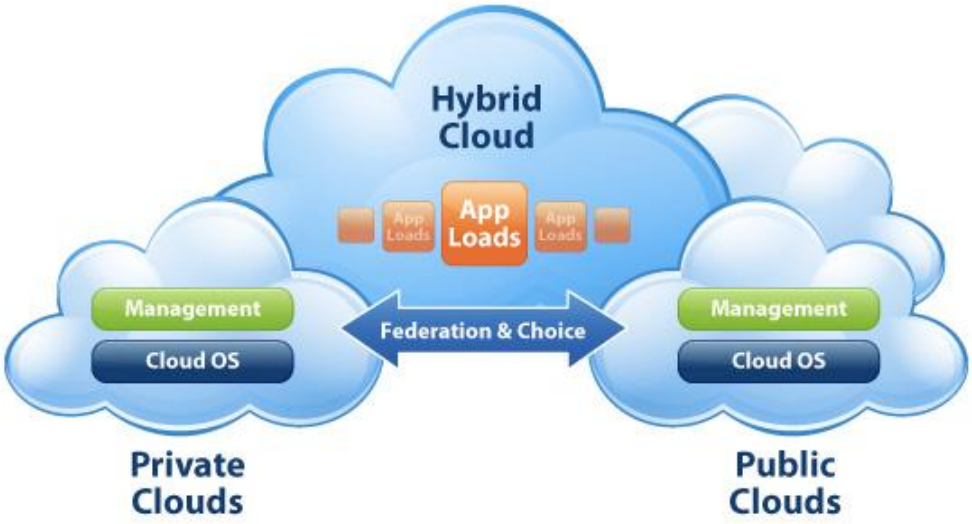

Ilustración 1 - Tipos de Nubes [3]

3.4 Community clouds

Este tipo de nubes no son tan comunes en la actualidad, pero es posible que crezcan en un futuro.

En este tipo de nubes existe una infraestructura comunitaria compartida entre una serie de entidades de una comunidad específica. Estas organizaciones suelen tener unos intereses comunes, como pueden ser la calidad, la seguridad, el cumplimiento de una serie de normas o leyes, etc. A su vez, estas nubes pueden ser administradas y controladas internamente o por una tercera parte, al igual que pueden estar alojadas en las propias empresas o en un lugar externo a ellas.

Los costes asociados a las Community clouds son distribuidos entre un menor número de usuarios que si lo comparásemos con una nube pública, y entre un mayor número de clientes si lo comparamos con una nube privada. Esto es así porque teóricamente este tipo de nubes son utilizadas por varias organizaciones (frente a las nubes privadas que en principio solo son utilizadas por la propia empresa que administra la nube), pero no serán utilizadas por tantos usuarios finales como puede pasar con las nubes públicas.

En definitiva, este tipo de nubes, comunidad nube, pueden ser muy interesantes y provechosas para entidades que tengan unos requisitos similares. Así, teniendo una infraestructura común (teniendo en cuenta esos objetivos similares de las organizaciones) estas entidades se podrían beneficiar de gran parte de los beneficios que tiene el usar el modelo Cloud Computing.

A continuación se muestra una figura de cómo pueden ser este tipo de nubes.

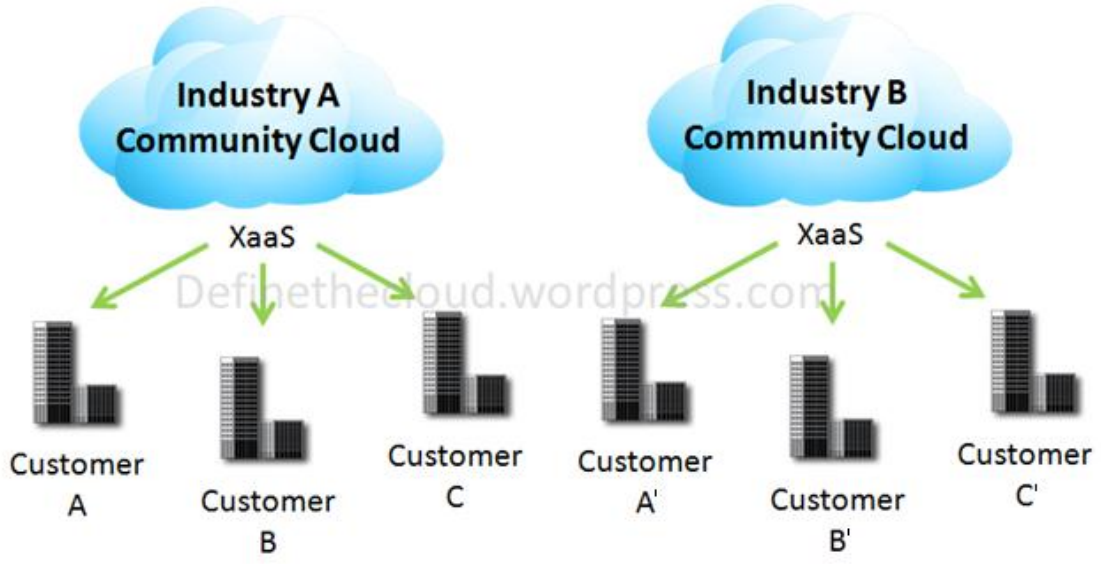

Ilustración 2 - Community Cloud [4]

En esta figura, tenemos 2 Community clouds, la Industry A, y la Industry B. Para cada nube comunidad, hay una serie de organizaciones que están dentro de esa nube, empresas que tendrán unos propósitos, requisitos y objetivos similares, para poder compartir una infraestructura cloud. Esas entidades en esta figura son customer A, customer B y customer C para la nube Industry A, y customer A´, customer B´, y customer C´ para la Community cloud Industry B.

Capítulo 4:

Capas

4.Capas

El modelo Cloud Computing se apoya en tres capas que no solo se encargan de encapsular los recursos demandados, sino que definen un nuevo modelo de desarrollo de aplicaciones. Además, dentro de cada capa, hay una gran variedad de opciones de negocios para definir los servicios que pueden ser presentados para su uso, es decir, que dentro de cada capa hay una serie de negocios específicos que se pueden llevar a cabo.

De esta manera, los proveedores ofrecen servicios que se agrupan en estas tres capas:

- Software como un servicio (del inglés *Software as a Service*, SaaS).
- Plataforma como un servicio (del inglés *Platform as a Service*, PaaS).
- Infraestructura como un servicio (del inglés *Infrastructure as a Service*, IaaS).

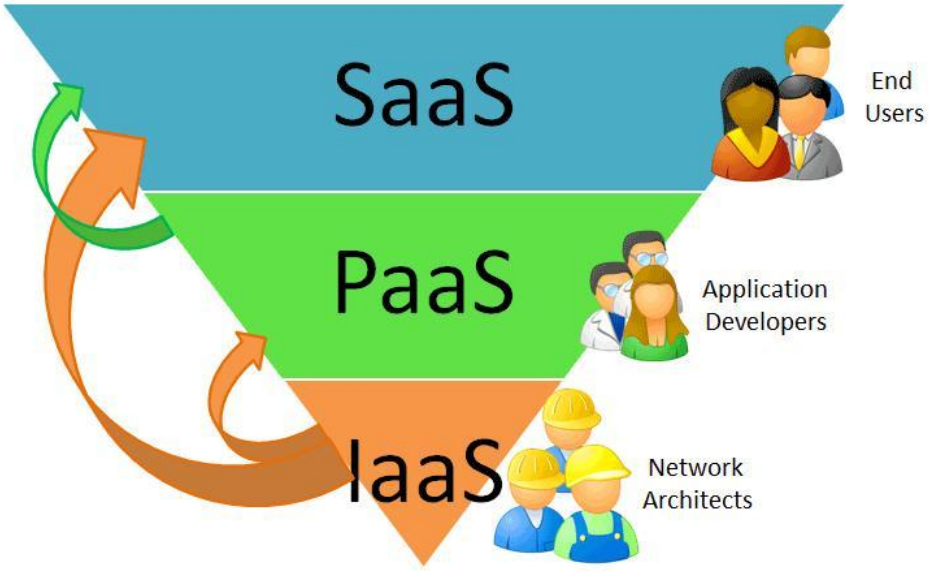

Ilustración 3 - Capas [5]

Como se puede observar en la figura, cada una de las capas se apoya sobre los niveles inferiores. Así, los servicios que se ofrecen en la capa SaaS, se soportan sobre la capa PaaS, y utilizan la infraestructura facilitada por la capa IaaS. Y de la misma manera, los servicios que se ofrecen en la capa PaaS se apoyan sobre la capa IaaS.

Poniendo un ejemplo, si en un momento dado una empresa contrata una serie de servicios de la capa SaaS de un proveedor de Cloud Computing, lo normal será que cuente con el soporte, actualización y mejora continua por parte de un equipo de desarrolladores que garantizan este mantenimiento de las aplicaciones. Asimismo, contará con la infraestructura necesaria para ejecutar dichas aplicaciones de la nube (servidores, ancho de banda, bases de datos, etc.). Aunque lo que realmente ocurre es que el cliente, a la hora de contratar los

servicios de la capa SaaS, también contrata de forma indirecta las prestaciones mencionadas anteriormente y pertenecientes a las capas PaaS y IaaS.

Por otra parte, estas tres capas dan como consecuencia tres tipos de clientes finales principalmente. Estos son:

- Empresas o usuarios finales que quieran contratar una serie de servicios software, que lo harán a través de servicios de la capa SaaS.

- Empresas o usuarios cuyo negocio o finalidad sea el desarrollo de software, para lo que necesitarán un entorno de desarrollo o programación, proporcionado por la capa PaaS.

- Empresas o usuarios que necesiten una ampliación de recursos hardware para llevar a cabo la finalidad de su negocio o propósito, lo cual lo proporcionará la capa IaaS.

A continuación vamos a pasar a detallar cada una de las tres capas definidas.

4.1 Software as a Service (SaaS)

Esta es la capa que más arriba se encuentra de las tres y, como hemos mencionado anteriormente, se alimenta de las capas inferiores *PaaS* e *IaaS*. Un primer acercamiento sería el de cambiar la idea de que las aplicaciones que hasta ahora han estado instaladas en una infraestructura propia (en local) ahora pasarán a estar alojadas en la nube.

Esta capa ofrece una variedad de servicios por parte del proveedor, que lleva consigo la utilización de la infraestructura y el mantenimiento del mismo suministrador de servicios software.

De esta manera, cuando un usuario o una entidad quiera contratar dichos servicios, podrá empezar a beneficiarse de ellos de forma inmediata (o casi), sin tener para ello que pagar licencias, ni dedicar parte de su propio hardware o personal para su puesta en marcha ni mantenimiento (porque como hemos dicho, el propio proveedor se encargará del mantenimiento, actualización, etc. del software que ofrece, y proporcionará su infraestructura para que las aplicaciones se ejecuten).

Un punto esencial de esta capa es que el catálogo de servicios y aplicaciones que se ofrecen ha de ser multi-tenencia. Esto es que las aplicaciones que ofrece un proveedor, han de poder ejecutarse en múltiples puntos, es decir, que han de poder utilizarla diversos usuarios finales, empresas o entidades.

El cliente, a la hora de utilizar el servicio contratado, accederá a él a través de un navegador Web, aunque desde su punto de vista será como si utilizase una herramienta más de su ordenador.

Por último, en esta capa SaaS, la forma de pago es por consumo, es decir, que se pagará solo por el volumen de utilización de los servicios ofrecidos.

Cabe destacar que los servicios que puede ofrecer esta capa de Computación en la nube serán útiles para aquellas empresas o entidades que no necesiten un software exclusivo para, por ejemplo, diferenciarse del resto de competidoras, o que utilicen un software muy específico por el tipo de negocio que lleven a

cabo. En este caso, la capa SaaS no resolvería sus problemas, puesto que lo que necesitarían sería un Software hecho a medida.

En contraposición, esta capa de Cloud Computing si que servirá a empresas o usuarios que utilicen el mismo software para realizar las tareas que normalmente llevan a cabo. Un ejemplo podría ser un software bursátil para empresas del sector financiero, ya que serviría a todo el gremio de empresas de ese sector.

Resumiendo, las principales características de la capa *Software as a Service* son:

- El acceso y la administración de los servicios ofrecidos por el proveedor de la nube se hacen a través de Internet.

- En lugar de lo que conocíamos hasta ahora donde cada usuario final tenía sus aplicaciones instaladas en su puesto de trabajo lo que conllevaba la necesidad poder acceder a ese terminal para poder utilizar dichas aplicaciones, en este modelo las aplicaciones se gestionan desde ubicaciones centrales, lo que permite tener acceso desde un navegador Web de forma remota.

- Como se ha mencionado con anterioridad, la distribución de los servicios y aplicaciones que ofrece la capa SaaS es multi-tenencia, en el que la aplicación se ejecuta en el proveedor (una única instancia), y es utilizada por múltiples usuarios finales.

- El conjunto de las actualizaciones que se realizan en las aplicaciones y servicios son centralizadas, por lo que los usuarios finales no tienen que descargarse ninguna actualización. Cada vez que utilicen los servicios

ofrecidos por el proveedor Cloud, estas aplicaciones llevarán las actualizaciones y modificaciones que se hayan realizado hasta el momento.

- Se paga solo por el volumen de utilización que se realiza de los servicios que se ofrecen, lo que se ha definido como pago por consumo.

En la tabla siguiente se pueden ver principales ventajas y desventajas de usar los servicios de la capa SaaS de Cloud Computing, algunas de ellas ya mencionadas:

VENTAJAS	DESVENTAJAS
• **Los costes se reducen y su riesgo también, puesto que se necesita una infraestructura ni un área concreta por parte del cliente final.** • **No se necesita comprar la licencia para el uso del software. Se paga el "alquiler" de la aplicación por el uso que se haga de los servicios.** • **El proveedor de Cloud Computing garantiza un servicio y atención al cliente 24 horas al día, los 365 días del año.** • **La propia empresa proveedora de servicios Cloud garantiza un acceso seguro a los entornos de las aplicaciones.**	• **Los clientes finales no tienen acceso directo a sus datos, ya que estos se encuentran en un lugar remoto, lo que podría generar problemas de control, seguridad, etc.** • **Lo que en principio es una ventaja al alquilar los servicios, conlleva que un usuario final no pueda realizar modificaciones sobre las aplicaciones.** • **Si en algún momento se rompiera la conexión a Internet o nos quedásemos sin él, la entidad o cliente final no podría acceder a las aplicaciones y, por lo tanto, no podría realizar las tareas que necesitase llevar a cabo.**

Tabla 1 - Software as a Service

4.2 Platform as a Service (PaaS)

Esta segunda capa se encuentra entre las capas SaaS y IaaS y, al igual que pasa con la capa SaaS, se alimenta de las capas inferiores, que en este caso solo es la capa IaaS.

Esta capa reúne y facilita una serie de funcionalidades que permiten crear y desplegar nuevas aplicaciones software. Normalmente estos nuevos servicios se implementarán para trabajar en entornos de Cloud Computing.

Las funcionalidades que integra la capa *Plataforma como Servicio* para llevar a cabo el fin definido son, por ejemplo, un entorno de desarrollo, una interfaz de programación de aplicaciones en uno o varios lenguajes, etc. De esta manera, la capa PaaS otorga todas las facilidades al programador para, entre otras cosas, analizar, desarrollar, prototipar, testear y probar, documentar y poner en funcionamiento las aplicaciones que se creen en este entorno.

Además, la infraestructura necesaria para poner esto en marcha la proporcionará el proveedor del entorno en nube en cuestión con su capa IaaS, como pasaba en la capa Software como Servicio.

Sin embargo, una de las posibles desventajas que puede tener es que cada capa PaaS de cada Cloud Computing tendrá un API de desarrollo (un grupo de rutinas que definen cómo invocar desde un programa un servicio que estos prestan, es decir, que representar una interfaz de comunicación entre componentes software), por lo que resultaría bastante costoso el mover una de estas aplicaciones creadas de un sistema Cloud Computing a otro.

Con todo ello, esta capa de Computación en la Nube tiene una gran variedad de ventajas, tales como:

- Arquitectura multi-usuario: Lo que significa que esta capa *Platform as a Service* da la capacidad al programador para que pueda tener la escalabilidad que necesite en cada momento del sistema.

- Las funcionalidades de análisis, desarrollo, prototipado, testeo y pruebas, documentación y puesta en funcionamiento se facilitan como servicio al cliente final en distintas combinaciones.

- Para que el desarrollo de las nuevas aplicaciones sea colaborativo, la capa PaaS tiene capacidad de que varios desarrolladores de la misma aplicación puedan compartir el código fuente, con un control de versiones, etc.

4.3 Infrastructure as a Service (IaaS)

La última capa es *Infraestructura como Servicio*, y se encuentra en el nivel más inferior de las tres capas que hemos visto. Por esta razón, esta capa no se alimentará ni se apoyará en ninguna otra, puesto que no tiene ninguna debajo de ella.

Esta capa ofrecerá unos servicios basados principalmente en proveer a clientes finales de servicios hardware, capacidades de cómputo, etc. Es decir, que el

proveedor de la capa IaaS permitirá utilizar recursos informáticos hardware a los clientes o entidades que contraten estas prestaciones dependiendo de las necesidades de estos en cada momento. Algunos ejemplos de recursos hardware podrían ser sistemas de almacenamiento, routers, servidores, etc.

Uno de las mayores ventajas que tiene es que las empresas o entidades que contraten estos servicios, podrán utilizar estos recursos hardware como si fueran suyos y los tuvieran físicamente, y podrán incrementar o reducir dichos recursos informáticos en un periodo muy pequeño de tiempo dependiendo de la demanda que puedan tener.

Poniendo un ejemplo, si una empresa tiene un pico de carga de trabajo que exige aumentar cierto número de recursos informáticos hardware, podrá contratar dichos servicios (o aumentarlos si ya los tiene contratados) a un proveedor de la capa *Infraestructura como Servicio* de Cloud Computing. Y, cuando ese pico de carga de trabajo termine, podrá volver al nivel normal que tiene establecido. Si este servicio por parte de la capa IaaS no estuviese disponible, la entidad o empresa tendría dos posibilidades ante tal problema: o bien no podría hacer frente a esa carga de trabajo, con las consecuencias para el negocio que podría tener en el presente y el futuro, o bien tendría que comprar la cantidad de hardware que necesitase, con su posterior instalación, configuración, etc. para poder hacer frente al problema, lo que le generaría un gasto que a largo plazo no llegaría a amortizar.

Otras ventajas que tiene la capa *Infraestructura como Servicio* son:

- El cliente final no tiene ni que mantener ni que configurar los recursos hardware contratados, ya que ese trabajo lo realiza el proveedor de servicios de Cloud Computing.

- Como ya se ha mencionado con anterioridad, se podrán aumentar los recursos informáticos hardware bajo demanda del cliente, por lo que será altamente escalable.

Capítulo 5:

Virtualización

5. Virtualización

El término Virtualización se puede definir como la creación por medio de software de algún dispositivo o recurso tecnológico como por ejemplo un sistema operativo, un servidor, un dispositivo de almacenamiento, una plataforma hardware. Además, todos los recursos de los que se disponga, así como todas las aplicaciones y usuarios podrán interactuar con los recursos virtualizados como si se tratara de recursos físicamente reales.

Un ejemplo muy simple de virtualización puede ser particionar un disco duro, ya que a partir de un solo disco podemos crear, por medio de simulación, 2 o más partes de un disco duro. Así, a simple vista parece que hay 2 o más discos duros físicos, cuando en realidad solo hay uno.

A continuación se muestra una figura con la que se puede entender de forma más sencilla este concepto.

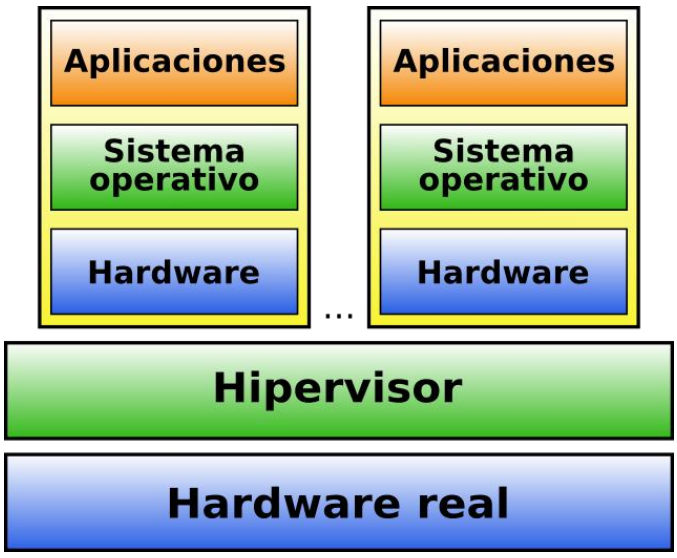

Ilustración 4 – Virtualización [6]

En esta figura se ve como utilizando la virtualización, desde una máquina física podemos ejecutar varias máquinas virtuales, cada una de ellas con el sistema operativo que se precise, así como poner en marcha las aplicaciones y recursos que se necesiten para cada máquina virtualizada.

En la figura podemos observar un rectángulo verde con el nombre *Hipervisor*. Este elemento, también denominado *Virtual Machine Monitor* (*VMM*), es una capa software encargada de manejar, gestionar y arbitrar los recursos principales de la máquina real. Estos recursos son: CPU, memoria, almacenamiento y conexiones de red. Esto permite ejecutar varias máquinas virtuales sobre el único hardware con el que cuenta la máquina real física, y es donde el *Hipervisor* o *VMM* se encarga de repartir de forma dinámica dichos recursos entre las máquinas virtuales que se están ejecutando.

Además de lo descrito, la virtualización permite ejecutar aplicaciones en cada máquina virtualizada. Es decir, que se puede hacer un uso de las máquinas virtuales como si fueran reales, pero siempre con las limitaciones que tenga la máquina física y de los recursos que asigne el *Hipervisor* a nuestras máquinas virtuales.

En la figura siguiente se muestra un ejemplo mucho más fácil de entender a simple vista, y más después de haber visto la figura anterior.

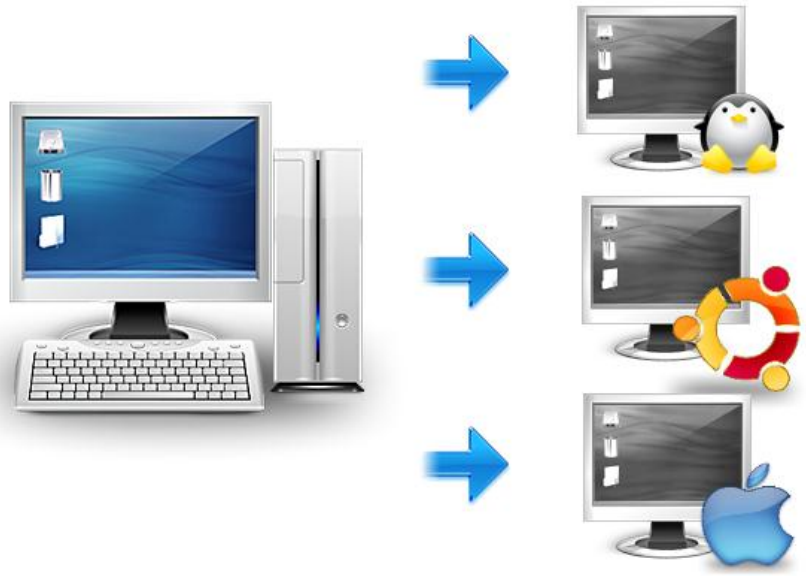

Ilustración 5 - Virtualización 2 [7]

En esta figura podemos ver cómo a partir de una máquina física, podemos ejecutar varias máquinas virtuales, con la posibilidad de ejecutar en cada una de ellas el sistema operativo que consideremos necesario. En la figura se están ejecutando tres máquinas virtuales sobre la misma máquina física. En la primera máquina virtual se está ejecutando una distribución de Linux, en la segunda una distribución de Ubuntu (que en realidad es también un Linux) y en la tercera se ejecuta Macintosh.

5.1 Características

A continuación vamos a pasar a detallar las características y ventajas que tiene la virtualización. Estas son:

- Se consigue una reducción de costes de IT (Tecnologías de la Información) gracias al aumento de la flexibilidad y eficiencia en el uso de los recursos que se tienen.

- Se tiene una administración global y centralizada de recursos, hardware, etc.

- Para las empresas y organizaciones la virtualización permite gestionar su CPD (Centro de Procesamiento de Datos) como un conjunto o agrupación de recursos comunes y de toda la capacidad de procesamiento, red, almacenamiento y memoria disponible en la infraestructura de las entidades.

- Gracias a la mejora de los procesos de copia y clonación de sistemas existentes, la virtualización facilita la creación de entornos de prueba para la puesta en marcha de nuevas aplicaciones o servicios, sin poner en riesgo todo el sistema que ya está en producción. Esto tiene como consecuencia que se tenga una mayor agilidad en el proceso de pruebas de las aplicaciones.

- Una de las características más importantes es el aislamiento. Esto garantiza que en caso de que haya un fallo en un sistema de una máquina virtual, este no afecte al resto de sistemas y máquinas virtuales que se tengan.

- Aparte de los beneficios directos que implican la reducción del hardware que se necesita, también se obtiene rentabilidad de los costes asociados a estos.

- Se puede realizar una migración mientras que las máquinas virtuales están activas de un servidor físico a otro sin perder el servicio. Con esto se consigue evitar la necesidad de paradas por mantenimiento en los servidores.

- Se hace una reutilización de hardware existente para utilización de software más actualizado, además de la optimización del aprovechamiento de los recursos hardware presentes.

- Se obtiene una mejora de los siguientes conceptos:

    - Del *TCO* (del inglés *Total Cost of Ownership*, que es un método para calcular los costes directos e indirectos, así como los beneficios asociados a la compra de equipos y/o programas informáticos).
    - Del *ROI* (que se trata de un ratio que compara el beneficio o utilidad obtenida en relación a una inversión realizada con anterioridad).

- Reduce los tiempos de parada del servicio.

- Se produce una contribución al medio ambiente gracias al menor consumo de energía derivado de menor utilización de servidores físicos.

5.2 Tipos de virtualización

A continuación se definen brevemente los distintos tipos de virtualización que se conocen hoy en día:

- Virtualización de almacenamiento: Este tipo de virtualización es normalmente usado en redes de área de almacenamiento, y se trata de la unión de varios dispositivos de almacenamiento para que simulen que se tiene una única unidad en lugar de múltiples.

- Virtualización de servidor: Se trata de la partición de un servidor físico en varios servidores virtuales. De esta forma, los recursos del servidor físico no son accesibles por los usuarios, y es el software el encargado tanto de dividir el servidor en múltiples virtuales como asignar dichos recursos.

- Virtualización de sistema operativo: En este tipo de virtualización, el servidor físico y una sola instancia del sistema operativo son virtualizados en multitud de particiones aisladas unas de otras. Cada una de estas particiones duplica un servidor real. El kernel (núcleo) del sistema operativo se ejecuta en un único sistema operativo, el cual luego provee a cada una de las particiones que se tengan.

- Particionamiento: Como en el ejemplo que se ha puesto al comienzo de este punto, el particionamiento consiste en la división de un recurso generalmente grande, como por ejemplo espacio de disco o ancho de banda de red, en recursos más pequeños que serán más fáciles de usar.

- Virtualización de aplicación: Este tipo de virtualización se encarga de separar las distintas aplicaciones de un sistema operativo. Transforma las aplicaciones que tenemos en servicios virtuales que son administrados y gestionados de forma centralizada. Una de las ventajas de este tipo de virtualización es que al ejecutarse en una máquina cliente (máquina virtual), se disminuyen o incluso se eliminan los conflictos que pueda haber con el sistema operativo o con otras aplicaciones.

- Virtualización de redes: Consiste en la partición lógica de una única red física para el uso de recursos de red. Se necesita la instalación de software y servicios para poder gestionar el almacenamiento compartido, los ciclos de computación y las aplicaciones. Este tipo de virtualización trata como un único grupo de recursos al conjunto de servidores y servicios de red, a los cuales se puede acceder.

5.3 Sistemas de virtualización

Existen multitud de sistemas que realizan el trabajo de virtualización. A continuación se nombra una pequeña muestra de los más conocidos en la actualidad, alguno de los cuales será nombrado más veces a lo largo del presente documento.

5.3.1 Hyper-V

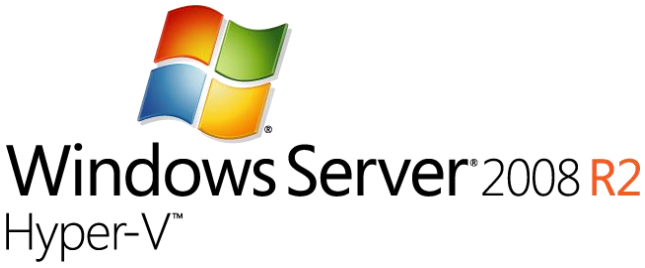

Ilustración 6 - Hyper-V [8]

Es el sistema de virtualización más actual de Microsoft. Se trata de una plataforma fiable y robusta que permite la virtualización de infraestructuras de IT. Permite virtualizar cualquier sistema operativo (tanto Linux como Windows), se tiene acceso a las shells de dichos sistemas operativos aunque no tengamos conexión de red en las máquinas virtuales, etc.

En contraposición, no podemos utilizar máquinas antiguas debido a que el nodo hardware tiene que soportar 64 bits (no soporta 32 bits) además de que para sistemas que no sean Microsoft se depende de este para que desarrollen herramientas de integración con Hyper-V.

5.3.2 VMware

Ilustración 7 – Vmware [9]

Es el sistema de virtualización más consolidado y uno de los más usados a nivel mundial. Se caracteriza por la facilidad a la hora de mover entornos virtuales entre distintos nodos incluso a escritorios para la realización de pruebas, entre otras cosas. Cuenta con una comunidad muy grande de desarrolladores, lo que facilita la administración ya que en Internet se pueden encontrar scripts para realizar multitud de operaciones engorrosas.

5.3.3 XenServer

Ilustración 8 - Xen Server [10]

Se trata del sistema de virtualización de Citrix (Citrix es una corporación multinacional que suministra tecnologías de virtualización e informática en la nube entre los que se cuentan los productos Xen de código abierto). Se trata de un sistema muy robusto que nos permite virtualizar casi todo, además de que la versión de Citrix proporciona una serie de herramientas tales como el XenCenter que facilita la gestión. Al igual que Hyper-V, se dispone de una consola con la que podemos acceder a los escritorios y a las shells aunque no dispongamos de conexión de red en las máquinas. El principal inconveniente de utilizar este sistema viene del precio, porque aunque tenga una versión gratuita, las características y funcionalidades más interesantes están en su versión de pago.

5.3.4 VirtualBox

Ilustración 9 – VirtualBox [11]

Oracle VM VirtualBox es un software de virtualización desarrollado por Oracle Corporation. Dentro de los productos de virtualización que posee Oracle, este es el más conocido y utilizado. Dentro de las ventajas que tiene están que virtualiza gran cantidad de sistemas operativos en distintas versiones, que es compatible para Windows, Linux y Mac OS, o que es muy estable a la hora de virtualizar el sistema operativo. Por otra parte, tiene desventajas como que no reconoce algunas distribuciones de Linux que no son tan conocidas.

5.3.5 Otros

Otros sistemas de virtualización pueden ser los siguientes: Mac-on-Linux, Microsoft Virtual PC, Virtual Iron, Adeos, Parallels Desktop, etc.

5.4 Papel de la virtualización en Cloud Computing

Con lo visto hasta ahora sobre la virtualización, podemos decir que es un punto de vital importancia en el mundo del Cloud Computing. Si bien no es imprescindible el virtualizar a la hora de pasarse a la nube, es recomendable y se utiliza siempre ya que ayuda en muchos aspectos, tales como tener unas infraestructuras más ágiles y flexibles, hace que sea más fácil adaptarse a las necesidades del negocio en cada momento, se pueden compartir recursos pudiendo ampliarlos o reducirlos según se necesiten, etc.

Por esta razón se puede decir que la virtualización es la piedra angular de las arquitecturas Cloud Computing en cuanto al diseño se refiere. En cuanto al papel de encapsulación de recursos físicos que tiene la virtualización en la computación en la nube, algunos de los puntos que resuelve y ventajas que tiene son los que siguen a continuación:

- Índices de utilización de los recursos más altos: Antes de la virtualización el uso medio de servidores, almacenamiento, etc. en los CPD (Centro de Procesamiento de Datos) de las empresas promediaba menos del 50%. Con la virtualización, las distintas cargas de trabajo pueden ser transferidas a sistemas sin uso o inactivos, con lo que se consolidan los sistemas que se tienen y se evitan compras innecesarias.

- Consolidación de los recursos: La virtualización favorece el fortalecimiento de gran cantidad de recursos de TI. Con la virtualización se pueden consolidar puntos tales como la arquitectura de sistemas, la

infraestructura de aplicación, los datos y bases de datos, redes, escritorios, etc.

- Uso y coste menor de energía: Debido a la subida del precio de la utilización de la energía, la virtualización posibilita el cortar y reducir el consumo total de energía que se utiliza (comparándolo con el uso de energía que se utilizaba antes de la virtualización), pudiendo ahorrar significativamente en este tipo de costes.

- Ahorro de espacio: Con la virtualización se puede ahorrar mucho espacio en servidores físicos, ya que se cuenta con los servidores virtuales que se tienen por cada servidor físico que posee la entidad. De no ser por la virtualización, se tendría que tener un amplio espacio para poder guardar y administrar el número de servidores físicos que actualmente ya no se necesitan porque se tienen virtualizados.

- Recuperación frente a desastre (continuidad del negocio): La virtualización facilita nuevas opciones de soluciones para la recuperación frente a desastres.

- Costes de operación reducidos: Antes de la virtualización se gastaba una gran cantidad de dinero en mantenimiento de la inversión de infraestructura realizada. Con la virtualización se puede reducir gran parte de la totalidad de ese gasto.

Por último, y como aclaración, cabe mencionar el hecho de que Cloud Computing y Virtualización son dos conceptos diferentes. No obstante, y como hemos visto a lo largo de este punto, la nube se apoya y se alimenta de la

virtualización, por eso que la virtualización juegue un papel muy importante en el Cloud Computing.

Capítulo 6:

Sistemas Cloud Computing utilizados en la actualidad

6. Sistemas Cloud Computing utilizados en la actualidad

En capítulos anteriores hemos visto que existen tres capas en el modelo Cloud Computing, en las cuales se encapsulan tres posibles negocios que pueden demandar las entidades o clientes finales de la nube.

Teniendo en cuenta todo lo visto hasta ahora, vamos a pasar a ver diversos ejemplos que existen en la actualidad de empresas que ofrecen servicios pertenecientes a cada una de las tres capas vistas: Software como servicio, Plataforma como servicio e Infraestructura como servicio.

6.1 Empresas de la capa SaaS

En este punto vamos a ver algunos ejemplos de empresas que existen actualmente que ofrecen los servicios de la capa SaaS de la nube.

6.1.1 Salesforce.com

Ilustración 10 – Salesforce [12]

Salesforce.com es una empresa multinacional de software empresarial que tiene su sede en San Francisco, Estados Unidos. Fue fundada en 1999 como una empresa especializada en software como servicio (SaaS), donde tres desarrolladores escribieron el software de automatización inicial de venta.

En 2004 la compañía entró a cotizar en la bolsa de Nueva York bajo el símbolo CMR (producto de la empresa consistente en la gestión de la relación con el cliente), aumentando sus ganancias hasta los 110 millones de dólares.

Desde el punto de vista del negocio, la propia entidad se vende como una empresa de Cloud Computing para empresas, donde se proporciona lo que el cliente final puede necesitar para gestionar las ventas y el servicio con el simple uso de un navegador. Todo esto se basa en la arquitectura multiusuario en tiempo real con la que cuenta el proveedor salesforce.com, que junto con su plataforma y las aplicaciones CRM (definido previamente como los servicios que ofrece la empresa) que tiene han conseguido revolucionar la forma en la que las empresas colaboran y se comunican con sus clientes.

Los servicios CRM que ofrece son varios. A continuación vamos a ver cada uno de ellos:

- Sales Cloud: Es una aplicación de ventas, que ofrece a representantes, gestores y ejecutivos todo lo necesario para conectar con los clientes y centrarse en lo que les sea más importante, que es más ventas y menos administración.

  Suministra herramientas de ventas, acceso a candidatos, cuentas de clientes, contactos, posibles negociaciones en curso que se puedan tener,

informes y paneles para analizar algo en concreto. En este servicio también se tiene una nueva forma de colaboración denominada *Chatter* por la salesforce.com, donde se pueden ver noticias en tiempo real, hacer un seguimiento de personas, documentos y proyectos que puedan interesar, es decir, una red social privada para los empleados. Además, en el centro de la página principal se obtiene la información más importante a través de paneles, que ofrecen una perspectiva en tiempo real de la situación y rendimiento del negocio que se lleva a cabo por la empresa que alquila los servicios de salesforce.com. También se tienen las próximas tareas y reuniones y, al poder sincronizarse con Outlook, Lotus notes y Google Apps, se tiene acceso a todo desde el propio servicio Sales Cloud.

Con todo esto, la entidad dedica su tiempo a lo que realmente es más importante en lugar de tener que buscar y recopilar información, con lo que potencia al máximo sus ventas.

Cabe decir que se puede acceder y estar conectado al negocio desde cualquier terminal móvil, ya sea a Sales Force como a Chatter, por lo que el usuario de Sales Force puede estar al tanto de todo en cualquier lugar siempre que tenga un teléfono móvil.

- Data.com: Este es también un servicio integrado en Sales Force, que sirve para llegar a las personas y clientes correctos, para centrarse en los objetivos y planificar territorios con datos altamente precisos de cuentas y contactos. Este servicio también contribuye a potenciar las ventas de una compañía.

- Radian6: Es un software que supervisa las redes sociales (Twitter, Facebook, Youtube, etc.) y que sirve para escuchar, medir y participar con los clientes en las mismas. Radian6 hace un glosario de la

información encontrada de la empresa, de la industria de la empresa, o de los competidores de la empresa, y los aglomera de tal manera que no tienes que andar buscando esa información en la red. Después, al tener toda esa información a tu disposición, puedes utilizarla en tu negocio.

- Service Cloud: Es un servicio de atención al cliente moderno, está completamente basado en la nube y sirve para satisfacer todas las necesidades y resolver todos los problemas del cliente. Al ejecutarse en la nube, solo hace falta iniciar sesión en SalesForce.com para poder beneficiarse de todos sus servicios.

6.1.2 Google Apps

Ilustración 11 - Google Apps [13]

Google Apps es un servicio de Google que ofrece de manera independiente las versiones personalizadas de varios productos de Google con un nombre de dominio personalizado. Tiene una serie de aplicaciones Web con funciones

similares a las tradicionales que se tenían en ofimática: Gmail, Google Groups, Google Calendar, Google Talk, Google Docs, Google Sites, etc.

Dentro de la historia de Google Apps cabe destacar un par de momentos importantes:

- El primero es cuando en octubre de 2007, Google adquirió la empresa Postini, centrada en temas relacionados con la seguridad del correo electrónico y la Web. Además, ofrece servicios Cloud Computing para el filtrado de correo electrónico *spam* y *malware* antes de su entrega al servidor del correo del cliente.

- El segundo es cuando en Marzo de 2010 Google lanzó Google Apps Marketplace, un sitio Web de aplicaciones para terceros basadas en la nube, cuya finalidad es completar las aplicaciones de Google ya disponibles. Se podría decir que es una tienda virtual para el usuario de Google Apps, donde se ofrecen aplicaciones tanto gratuitas como de pago.

Con todo esto, dentro de Google Apps se pueden diferenciar 3 ediciones. Estas son: Google Apps (edición gratuita), Google Apps for Business y Google Apps for Education. En la siguiente tabla se puede ver un resumen de los servicios y funcionalidades de cada una de las tres ediciones:

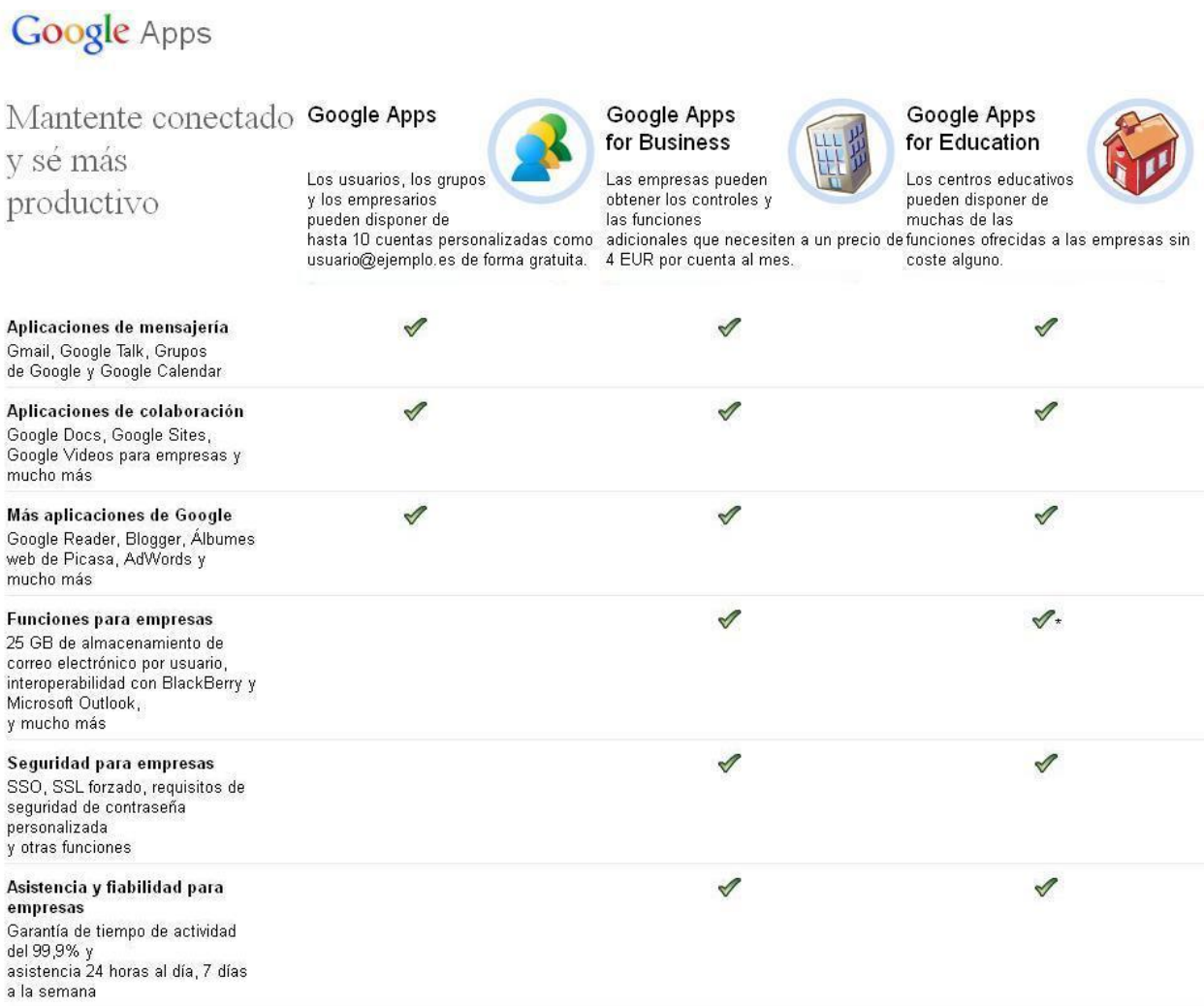

Ilustración 12 - Google Apps 2 [14]

Algunos ejemplos de entidades que usan la edición Business o Education son las siguientes:

- Google Apps for Business: BBVA (que ha empezado a utilizar los servicios de Google Apps a principios de este año 2012), Jaguar Land Rover, IRB Barcelona (Instituto de investigación biomédica), Grupo Boyacá o El Servicio Extremeño Público de Empleo (SEXPE).

- Google Apps for Education: Universidad de Notre Dame (Francia), Universidad de Westminster (Inglaterra), Trinity College Dublín

(Irlanda), Universidad Rey Juan Carlos de Madrid (España) o Universidad de Granada (España).

Dentro de Google Apps for Business, existe un servicio denominado Google Cloud Connect para Microsoft Office el cual permite la posibilidad de edición en colaboración de varios usuarios del conocido software Microsoft Office, el cual posibilita compartir y modificar de forma simultánea documentos de Microsoft Word, PowerPoint y Excel con tus compañeros de trabajo, así como realizar copias de seguridad.

6.1.3 iCloud (Apple)

Ilustración 13 – iCloud [15]

iCloud es un servicio que lanzó la empresa Apple en junio de 2011. Este software permite a los usuarios, mediante los diferentes dispositivos de dicha marca (Iphone, Ipod, Ipad, etc.) que todos los datos, tales como archivos de música, fotografías, datos del calendario, correo electrónico, etc. se almacenen en servidores remotos, de manera que si una persona realiza una fotografía, da

de alta una nueva reunión en su calendario, recibe un nuevo email, etc. todos esos cambios estarán disponibles en el momento en que acceda a cualquiera de sus otros terminales de la marca Apple (y como excepción, a equipos sistemas operativos Windows Vista o más recientes). Es decir, que hay una sincronización del correo electrónico, contactos, calendarios, marcadores, notas, listas de tareas, música, fotos, etc. entre todos los terminales Apple que posea un cliente determinado.

Además de esto, iCloud tiene las siguientes características:

- Permite hacer copias de seguridad de los dispositivos iOS (sistema operativo de iPhone) en línea, además de poner restaurar una copia de seguridad sin necesidad de conectar el terminar a ningún equipo.

- Permite rastrear la ubicación del iPhone, iPodTouch o iPad del cliente, mostrando en un mapa su posición. Además, permite emitir un sonido (aún si está en modo silencio), cambiar la contraseña del dispositivo o incluso borrar la información que contenga de forma remota.

- Posibilita desde un dispositivo Apple el acceso remoto a otros ordenadores cuya configuración sea el mismo ID de Apple que el terminal desde el que se accede.

En resumen, el servicio Cloud está integrado en las distintas aplicaciones (itunes, fotos, documentos, Apps, libros y copias de seguridad, calendario, mail y contactos, etc.) y dispositivos, con el requisito indispensable de que los terminales han de tener instalado el sistema operativo iOS 5 en el caso de iPhone, iPad o iPod touch, el sistema operativo OS X Lion en el caso de tener un

Mac, o el sistema operativo Windows vista o más reciente en el caso de que sea PC.

6.1.4 Microsoft Office 365

Ilustración 14 - Office 365 [16]

En octubre de 2010 Microsoft Corporation anunciaba el lanzamiento de su nuevo servicio, Microsoft Office 365, la siguiente generación de sus productos, esta vez en la nube, aunque no estaría disponible a nivel mundial hasta el año pasado, 2011. De esta forma cambia el paradigma en que los usuarios y empresas hacen uso de las aplicaciones de Microsoft Office cambia, ya que a partir de ese momento no es necesario tener instalado dicho software en el equipo en que vayamos a trabajar, sino que partiendo de una suscripción online del servicio, se dispone de las diferentes prestaciones que ofrece Microsoft Office 365, y todo esto accesible desde casi cualquier terminal (Pc, móvil, tablet, etc.).

Las principales características y servicios que ofrece Microsoft Office 365 son los siguientes:

- Acceso a correo electrónico, calendarios desde cualquier equipo o terminal con acceso a Internet.

- Posibilidad de crear video conferencias en un momento.

- Se pueden crear, guardar y modificar documentos de Office (Word, PowerPoint, Excel, OneNote, etc.) online igual que antes los guardábamos en nuestro equipo.

- Uso compartido de archivos: se puede administrar el contenido compartirlo.

- Se puede crear un sitio Web para la empresa que contrata los servicios de Microsoft Office 365.

- Movilidad: Se pueden recuperar documentos, enviar y recibir emails, ver información sobre citas, etc. mediante dispositivos portátiles ya sean teléfonos móviles (Smartphones) o tablets.

Además, estos servicios están disponibles para cualquier tipo de empresa, sea cual sea su tamaño (desde pequeñas y medianas hasta grandes empresas).

Algunos ejemplos de empresas que en la actualidad usan los servicios de Microsoft Office 365 son, por sector:

- Servicios profesionales: Servicios Dell, HSS, Afirma Consulting o C&I Engineering.

- Manufacturación: Thomas Kemper Soda Company, PSI Solutions o Naturally Me.

- Educación: Universidad de Texas en San Antonio.

- Sin ánimo de lucro: All Saints Isleworth, The Wise Group o D&L Representative Payee Services

6.1.5 Zoho

Ilustración 15 – Zoho [17]

Zoho se denomina a un conjunto de aplicaciones Web creadas por la empresa "Zoho Corporation Private Limited". Zoho.com se trata de una división de esta empresa. Los servicios Web que ofrece requieren registrarse en su página Web. Además, tiene una versión gratuita para uso personal, y versiones de pago para entidades y empresas.

Gracias a las 22 aplicaciones Web que ya tiene disponibles, Zoho.com ha recibido premios tales como "Producto del año" en 2009 por la empresa InfoWorld, "Premio a uno de los 25 productos más innovadores" en 2008 por PC World, y "Mejor arranque de una empresa" en 2007 por TechCrunch.

Las aplicaciones que ofrece Zoho.com se dividen en 3 categorías: Aplicaciones de productividad, aplicaciones de colaboración y aplicaciones de negocio. Dentro de cada categoría, las características de las aplicaciones que ofrecen son las siguientes:

- Aplicaciones de Productividad:

    - Programar y gestionar reuniones, citas eficientemente con tu calendario.
    - Planificador con el que de forma sencilla puedes seguir tus citas.
    - Posibilidad de crear edita y compartir presentaciones online (Zoho Office for Microsoft SharePoint).
    - Crear y compartir hojas de cálculo (Zoho Viewer) y documentos de texto online.
    - Zoho plugin para Microsoft Office, para poder colaborar con Microsoft Office de forma cómoda.

- Aplicaciones de colaboración:

    - Chat con posibilidad de crear grupos de decisión, discusión de forma rápida y en tiempo real.
    - Posibilidad de crear, almacenar y mantener toda la documentación que quieras en un sitio centralizado.

- Lograr comunicaciones de negocios eficientes mediante e-mail.
- Gestionar y seguir varios proyectos online hacia un final exitoso.
- Wiki para compartición de conocimientos online.
- Repositorio público centralizado de documentos, pdf´s, etc.
- Posibilidad de mantener video conferencias y discusiones online.
- Medio para recopilar, administrar y priorizar la respuesta de los clientes

- Aplicaciones de Negocio:

  - Asistencia para conectar y arreglar problemas de forma remota.
  - Gestión y seguimiento online de las necesidades de Recursos Humanos.
  - Aplicación de facturas para que los pagos se hagan a tiempo.
  - Extracción de datos para identificar tendencias y más observaciones con facilidad.
  - Posibilidad de crear cuestionarios de forma rápida
  - Fácil gestión de las finanzas de forma segura.
  - CRMs (Gestión de la satisfacción de los clientes) para cerrar acuerdos de forma rápida.
  - Marketplace: para encontrar desarrolladores y soluciones para satisfacer las necesidades de tu negocio.
  - Monitorización de sitios Web en cualquier momento y en cualquier lugar.
  - Proveedor de atención al cliente de primera calidad online.

6.1.6 Empresas en el mercado español (SaaS)

A continuación vamos a describir ejemplos de empresas que ofrecen servicios de la capa Software como Servicio en el mercado español.

El listado de empresas se detalla a continuación:

- 1&1: Esta empresa proveedora de servicios ofrece una amplia variedad de soluciones SaaS. El producto más destacado es *1&1 Mi Web*, que permite y facilita a los clientes, a partir de diseños, textos e imágenes específicos (para más de 100 sectores diferentes), crear su propia página Web. Para el correo, 1&1 ofrece MS Exchange como el MailXchange. En adición, con las cuentas de correo, 1&1 proporciona disco duro online y aplicaciones office gratuitas.

- Aner: Este desarrollador comercializa novedosas soluciones de software online en modalidad SaaS para pymes. Entre ellas destacan *CRM online*, que es una herramienta para la realización y gestión de encuestas a través de Internet, y *Business Intelligence*, que facilita la visualización y el análisis de datos empresariales financieros y comerciales. Está diseñado para todo tipo de usuarios y es de fácil usabilidad. Además de estos servicios, Aner ofrece servicios de diseño y posicionamiento Web a pequeñas empresas, así como soluciones de movilidad, seguridad y comunicaciones.

- Arsys.es: Sobre todos los servicios que ofrece destaca WebMaker, una solución para la creación de páginas Web. Va dirigido a profesionales sin conocimientos de programación y diseño Web, para que en tres sencillos pasos puedan poner en marcha su sitio Web. El primer paso es elegir la

plantilla que más se ajuste al sector de la empresa u organización y a las necesidades de nuestro negocio (entre más de 100 categorías); el segundo paso es insertar los widgets que queremos en nuestra página Web; y el tercer y último paso es la edición de textos e imágenes que queremos que aparezcan en nuestro sitio Web. Aparte de WebMaker, cuenta con la solución Tiendas Online, que va dirigida a profesionales y organizaciones que quieran realizar e-commerce.

- Avantaas: Esta empresa de reciente creación ofrece soluciones en la nube a la distribución. Además, de VirtualSharp (que da servicios de respaldo), en el catálogo de Avantaas se pueden encontrar aplicaciones para escritorio virtual de Quest y soluciones para centro de datos virtual de VMware, Citrix y NetApp. Como se menciona al principio, al ser una empresa recién creada, está trabajando para ampliar su catálogo de servicios.

- Citrix: Entre otras cosas proporciona el acceso en modo servicio a soluciones *Desktop as a Service*, es decir, aplicaciones del entorno Windows como servicio como si estuvieran en tu propio escritorio de trabajo. Asimismo, ofrece soluciones nativas en la nube para clientes finales, como por ejemplo *ShareFile*, que facilita el almacenamiento centralizado en la nube permitiendo la compartición de archivos y el acceso a ellos desde cualquier parte. También ofrece servicios orientados a software colaborativo, como *Citrix On Line*, que incluyen acceso a dispositivos remotos (*GoToMyPC*), soporte remoto (*GoToAssist*) y soluciones de trabajo en grupo (*GoToMeeting* y *GoToWebminar*).

- Esker: Este desarrollador ayuda a las empresas a mejorar su rentabilidad eliminando la gestión manual de los documentos en papel. Ofrece este servicio como SaaS, que permite a las empresas acceder más fácilmente a las soluciones de automatización de procesos documentales. El catálogo con los principales servicios que ofrece Esker son los siguientes: Envíos de documentos, automatización de facturas de proveedores, de facturas a clientes y de pedidos de clientes.

- MakeSoft Technologies: Esta consultora cuenta con un gran catálogo de soluciones dentro de la capa Software como Servicio. Estos servicios que ofrece permiten a las entidades acceder a aplicaciones de gestión empresarial que optimizan su negocio sin la necesidad de realizar grandes inversiones iniciales, y pagando solo por lo que se usa en cada momento. Además, tiene una plataforma propia de máxima seguridad que cumple con la LOPD y ofrece varias líneas de negocio, como por ejemplo outsourcing y consultoría.

- Meta4: El servicio *Global HR SaaS* que ofrece este desarrollador es una plataforma que permite dar respuesta a todas las funciones y actividades del área de Recursos Humanos. Esto es la administración del personal, la gestión de la organización, la gestión estratégica del talento, etc. Este servicio está a disposición de las organizaciones y profesionales en modo alquiler, por lo que Meta4 se encarga de la inversión y mantenimiento de la tecnología, lo que supone un gran ahorro de costes para las empresas que utilicen este servicio.

- Primavera: La oferta actual de la que dispone este desarrollador incluye un amplio portfolio de soluciones ERP. Todas estas soluciones son modulares y totalmente integradas, por lo que contribuyen a la

optimización de la gestión empresarial en todos sus ámbitos: RRHH, contabilidad, compras, ventas, contabilidad, etc. Primavera también cuenta con soluciones verticales para el sector de la construcción e industria, y cuenta además con el servicio *Qpoint*, solución especializada para la gestión de procesos de calidad. A esta serie de servicios se le une un amplio paquete de soluciones de infraestructura, alojamiento, actualizaciones y bases de datos que completan la oferta de Primavera.

- Sage: Es una empresa dedicada al desarrollo software, cuya nueva propuesta de servicios en la nube va dirigida a pymes y autónomos. Cuenta con una serie de servicios que son gratuitos durante el primer mes y que posteriormente van por suscripción mensual. Además, incluyen un servicio de soporte vía *Sage Responde*, accesible desde el panel de servicios y desde cada una de las aplicaciones. Las aplicaciones que ofrece Sage en esta modalidad se describen a continuación:

    - *ContaOnline*, una herramienta Web para gestionar la contabilidad financiera.
    - *eFactura Online*, herramienta para realizar y gestionar facturas.

- Stonesoft: Se trata de un proveedor de soluciones de seguridad. Su servicio *A2cloud* garantiza la autentificación y un acceso seguro a la nube. Este servicio se ofrece como una combinación de otros dos servicios: *StoneGate Authentication Server*, con el que se consigue una autenticación robusta a través de la utilización de servidores basados en Radius (un protocolo de autenticación y autorización para aplicaciones de acceso a la red), y *StoneGate SSL VPN*, con el que se consigue un salto en la seguridad de acceso a aplicaciones gracias a las técnicas de autentificación multifactor y multimétodo que implementa.

- Telefónica: Esta operadora cuenta con una tienda online que contiene, entre otras cosas, aplicaciones de Telefónica. Esta tienda online se llama *Aplicateca*, y nació en 2009. Gracias a esta plataforma, Telefónica ofrece a las pymes herramientas para la ayuda en la gestión de flotas de vehículos, incidencias, contabilidad, programas de formación, RRHH, facturación, etc. En esta misma plataforma también se pueden encontrar soluciones y servicios de proveedores de Wolters Kluwer (Empresa editorial y de software que provee de información profesional a diferentes profesionales, tales como abogados, directivos de empresas, etc.) o de McAfee (que es una empresa que ofrece soluciones de seguridad frente a virus) entre otros.

- SaaS & Go: Esta empresa establecida en Barcelona ofrece un servicio a las empresas con gran multitud de funcionalidades. Este servicio se llama *Openbravo* y un servicio ERP (Planificador de Recursos empresariales). Las principales funcionalidades y módulos que ofrece Openbravo son:

    - Gestión de datos maestros (Productos, listas de materiales, clientes, proveedores, empleados, etc.).
    - Gestión de aprovisionamientos (Tarifas, pedidos de compra, recepción de mercancías, planificación de los aprovisionamientos, etc.).
    - Gestión de almacenes (Almacenes y ubicaciones, lotes, número de serie, etiquetas, entradas, salidas, inventarios, transportes, etc.).
    - Gestión de proyectos y servicios (Proyectos, tareas, fases, recursos, presupuestos, etc.).
    - Gestión comercial y CRM (Tarifas, pedidos de ventas, albaranes, CRM, etc).

  - Finanzas y contabilidad (cuentas contables, contabilidad general, cuentas a pagar, cuentas a cobrar, contabilidad bancaria, balance, cuenta de resultados, etc.).
  - Gestión de la producción (Estructura de planta, planes de producción, órdenes de fabricación, partes de trabajo, costes de producción, etc.).
  - Inteligencia del negocio (Informes, análisis, etc.).

- VMware: Esta empresa cuenta con una serie de soluciones de plataforma de aplicaciones de cloud abierta de VMware. Estas soluciones proporcionan una gran base para la creación, ejecución y gestión de aplicaciones virtuales modernas. Gracias a estos servicios se consigue una aceleración en la distribución de las aplicaciones actuales y futuras de la nube. Hoy en día más de dos millones de profesionales y desarrolladores confían en esta plataforma de aplicaciones cloud de VMware para llevar a cabo su propósito de tener servicios escalables, portátiles y dinámicos.

- Doscontrol: Esta empresa combina los servicios de hosting en la nube (*Cloud Hosting Online*) y la suscripción a los servicios de Sage (vistos con anterioridad). Gracias al alojamiento online en la nube, las operaciones como las copias de seguridad, administración de los sistemas, actualizaciones de las ERPs de Sage, etc. son realizadas en la nube, por lo que el cliente se puede despreocupar de ello.

- Vodafone: Esta operadora telefónica ofrece tanto a empresas como a autónomos un catálogo de servicios y aplicaciones en la nube. Dentro de este catálogo destacan algunas aplicaciones tales como Office 365 (de la que hemos hablado con detalle con anterioridad), aplicaciones

avanzadas de productividad (como ComuniTake, Works o NetDuo) o disco en red.

- Wolters Kluwer: A3 ERP\CRM Web es el servicio que ofrece esta empresa para las pymes que necesitan una herramienta potente para la gestión eficaz de sus acciones comerciales. Es una solución completamente cloud, y con ella el cliente puede disponer, con tan solo una conexión a Internet, de toda la información generada en las relaciones con sus clientes y de un seguimiento de las oportunidades de venta creadas. Con un solo clic se accede a los datos de los clientes de la empresa, lo que facilita la toma de decisiones comerciales de una forma muy ágil e intuitiva.

6.2 Empresas de la capa PaaS

Ahora vamos a ver algunos ejemplos de empresas que actualmente ofrecen los servicios de la capa PaaS de la nube.

6.2.1 Google App Engine

Ilustración 16 - Google App Engine [18]

Google App Engine, también conocido como GAE o App Engine, es un servicio de Google que nos proporciona la infraestructura de producción de Google de forma gratuita como plataforma de desarrollo y hospedaje de aplicaciones Web.

Su lanzamiento fue a principios de abril de 2008 como un servicio en la nube de Plataforma como Servicio (PaaS).

Las aplicaciones App Engine son fáciles de crear, mantener y de ampliar en el caso de que pueda ir aumentando el tráfico de la misma y las necesidades de almacenamiento de datos. Además, no hace falta la utilización de ningún servidor para que funcione la aplicación, solo es necesario subirla para que se pueda empezar a usar.

A estas aplicaciones que se crean se les puede dar el dominio que uno quiera a través de Google Apps (visto como uno de los ejemplos del apartado anterior: Empresas de la capa SaaS), y también se les puede asignar un nombre siempre y cuando esté disponible en el dominio *appspot.com*. Además, existe la posibilidad

de compartir la aplicación con un número limitado de usuarios o con todo el mundo, según se prefiera o necesite.

Uno de los puntos más importantes es el número de lenguajes de programación que admite Google App Engine. Cuenta con un entorno de tiempo de ejecución Java de App Engine y con un entorno de tiempo de ejecución Python dedicado:

- El entorno de tiempo de ejecución Java te permite crear aplicaciones a través de tecnologías Java estándar o a través de cualquier lenguaje que utilice un intérprete o compilador basado en *Java Virtual Machine* (*JVM*), como por ejemplo JavaScript.

- El entorno de tiempo de ejecución Python dedicado incluye un intérprete de Python y la biblioteca estándar Python.

Cabe decir que ambos se generan para garantizar que las aplicaciones se ejecutan de forma rápida, segura y sin interferencias de otras aplicaciones en el sistema.

La forma de pago de Google App Engine es gratuita a la hora de empezar a utilizarlo. Todas las aplicaciones tienen 500 MB de almacenamiento y suficiente CPU y ancho de banda que permiten un servicio eficaz de unos cinco millones de visitas a la página al mes sin coste alguno. En el momento que el usuario habilita la facturación para su aplicación, se incrementan los límites gratuitos comentados anteriormente y solo se paga por los recursos utilizados por encima de los servicios gratuitos que se ofrecen.

En cuanto al entorno de aplicación de GAE, este incluye una serie de funciones detalladas a continuación:

- Servidor Web dinámico compatible con las tecnologías Web más comunes.

- Servicio de almacenamiento continuo con funciones de consulta, clasificación y transacción.

- Distribución de carga y escalado automático.

- API (del inglés Application Program Interface) para autenticar usuarios y enviar e-mails a través de Google Accounts.

- Entorno de desarrollo local completo simulado por App Engine en el equipo del usuario.

- Colas de tareas que realizan trabajos fuera del ámbito de una solicitud Web.

- Tareas programadas para activar eventos en momentos determinados y en intervalos regulares.

Con todas estas funciones, las aplicaciones se pueden ejecutar en cualquiera de los dos entornos de tiempo de ejecución descritos anteriormente, donde ambos proporcionan protocolos y tecnologías comunes para el desarrollo de aplicaciones Web.

Además de todo esto, el entorno de aplicación cuenta con una zona de pruebas. Esta zona de pruebas hace que las aplicaciones se ejecuten en un entorno seguro y que limiten el acceso al sistema operativo subyacente, lo que permite a App Engine distribuir peticiones Web de la aplicación en varios servidores, y detener o iniciar dichos servidores según las demandas de tráfico de la aplicación. En adición, la zona de pruebas aísla la aplicación en su propio entorno seguro de confianza, que es totalmente independiente de hardware, sistema operativo y ubicación física del servidor en el que se ejecute.

Igualmente, el entorno de aplicación proporciona un potente almacén de datos que incluye motor de búsqueda y transacciones, y que crece de forma proporcional al crecer el servidor Web distribuido cuando crece el tráfico.

Algunos ejemplos de empresas y/o aplicaciones que utilizan Google App Engine para su negocio son las siguientes:

- LifeAware: Es una aplicación móvil de la empresa del mismo nombre para plataformas iPhone y Android. Permite compartir, no solo tu ubicación con los amigos que hayas autorizado, sino también configurar zonas para que se te notifique cuando tus amigos entren en ellas o las abandonen. Puedes especificar zonas como el colegio o el lugar de trabajo.

- GigaPan: es una aplicación Web compuesta por tres avances tecnológicos: una base de cámara robótica, un software de edición de imágenes y un nuevo tipo de sitio Web llamado "Gigapan.org", al que se puede acceder para compartir y comentar sobre todo lo relacionado con las vistas panorámicas en gigapíxeles y con los detalles que en ellas se incluyen. Usa Google App Engine en su sitio Web, publica imágenes de

varios gigapíxeles en Google Earth, permite la ubicación y orientación de dichas imágenes en Google Earth, etc.

- Socialwok: es una aplicación que ofrece funciones empresariales de uso compartido y colaboración basadas en alimentación para la plataforma de Google Apps. Las entidades o empresas pueden usar sus cuentas existentes en Google Apps para acceder a Socialwok y crear una red social en sus dominios que les permita compartir elementos de Google Calendar, Google Docs, etc. Utiliza App Engine para Java para hacer llegar nuestro servicio Web a usuarios de móviles y al público en Internet.

6.2.2 Force.com y Heroku

En el punto 4.1.1. hemos visto un proveedor SaaS, salesforce.com. En esta misma empresa se tiene la posibilidad de crear aplicaciones.

Consta de dos servicios principales, uno específico para crear aplicaciones para los empleados de una empresa o entidad, y otro específico para crear aplicaciones de cara al cliente final. Cabe decir que ambos servicios se integran en el mismo sistema.

Ilustración 17 - Force.com & Heroku [19]

6.2.2.1 Force.com

Primero vamos a ver el servicio para crear aplicaciones para los empleados de una empresa, que se llama force.com.

Ilustración 18 - Force.com [20]

Force.com es el servicio enfocado para crear aplicaciones para los empleados tales como aplicaciones para departamentos concretos (recursos humanos, contabilidad…), procesos comerciales, etc. Para ello cuenta con una plataforma de desarrollo para crear estas aplicaciones fácilmente (con todos los servicios necesarios disponibles e integrados). Se trata de un desarrollo visual cuyo diseño consiste en arrastrar y soltar, y cuenta con varias APIs que hacen más sencilla la conexión con otras aplicaciones ya existentes. Además, cada

aplicación cuenta con funcionalidad integrada para redes sociales y movilidad, que es un punto muy importante ya que se pueden acceder a dichas aplicaciones desde un navegador Web o un dispositivo móvil.

Para aplicaciones que requieran requisitos más complejos, Force.com cuenta con herramientas para desarrolladores profesionales tales como lenguajes de programación, entornos de desarrollo y pruebas, integración de control de recursos para desarrollo en equipo, etc.

Algunos clientes de Force.com son *Facebook* (red social), *Kelly Services* (empresa que ofrece servicios de personal temporal, subcontratación, personal a tiempo completo, etc.) o *Qualcom* (compañía estadounidense productora de chipsets para tecnología móvil y responsable del cliente de correo electrónico Eudora).

Los productos que componen Force.com son los siguientes:

- Appforce: facilita la creación de nuevas aplicaciones (se pueden crear cinco veces más rápido y aproximadamente a la mitad del coste de las plataformas software tradicionales). Se pueden crear aplicaciones con un porcentaje de clicks-programación de 80-20. Además, permite la ejecución de las aplicaciones en dispositivos móviles y permite a los usuarios crear sus propios informes y paneles.

- Site.com: Es un servicio para crear sitios Web orientados a datos para el negocio de una entidad o empresa. Site.com incluye el alojamiento de sitios Web, la gestión de contenidos, una base de datos y una red de entrega de contenidos.

- ISVforce (ISV viene de "Independent Software Vendor", es decir, compañías que producen software): proporciona una serie de herramientas y recursos necesarios para distribuir y comercializar aplicaciones. Es importante decir que más de 1000 proveedores de software independientes utilizan este producto para llegar a muchos más clientes.

- Database.com: Se trata de la base de datos sobre donde se apoya tanto Force.com como Heroku que veremos un poco más adelante. Esta base de datos facilita la creación de aplicaciones para su posterior acceso desde un dispositivo móvil y también da la capacidad de dotar a dichas aplicaciones de red social, con lo que se alcanzan nuevos niveles de colaboración y productividad (gracias a la capacidad de red social que nos da database.com).

6.2.2.2 Heroku

Ilustración 19 – Heroku [21]

Heroku es el servicio que ofrece salesforce.com para crear aplicaciones de cara al cliente.

Las principales características de este servicio son:

- Implementación ágil de los lenguajes de programación Ruby, Clojure, Python y Scala, y del entorno de programación Node.js. Además, te permite centrarte por completo el desarrollo del código ya que proporciona todo lo relacionado con servidores, instancias o máquinas virtuales.

- Posibilidad de ejecutar y ampliar cualquier tipo de aplicación: Se puede ejecutar cualquier Web o proceso en background independientemente del Framework de desarrollo; Se puede obtener el control de la aplicación y escalar los procesos de distribución; y es fácilmente escalable al número de usuarios que sea necesario.

- Completa visibilidad de la aplicación: Transparencia consolidada, registros y estado de cada componente de la aplicación en tiempo real, y desde Heroku se realiza el despliegue de la aplicación, el gestión de los procesos de la misma y rutas de tráfico.

- Arquitectura resistente y buenas superficies de control. Heroku se encarga de la salud y el buen funcionamiento de las aplicaciones por lo que el usuario no se tiene que preocupar de eso, solo tiene que centrarse en administrar y dirigir sus aplicaciones con la ayuda de un conjunto de APIs de control de superficie.

Cabe decir que en la actualidad hay casi 2.000.000 de aplicaciones ejecutándose en Heroku.

6.2.3 Windows Azure Platform

Ilustración 20 - Windows Azure [22]

Windows Azure Platform forma parte de los servicios online que ofrece Microsoft. Proporciona un entorno familiar y flexible para desarrollar aplicaciones y servicios en la nube de Microsoft, con todas las ventajas que esto conlleva. Así, la reducción de tiempo a la hora de lanzar nuevos productos y la fácil adaptabilidad a la demanda en cada momento crece considerablemente, ventajas que las entidades valoran.

Windows Azure es una plataforma la cual permite crear aplicaciones y productos en diversos lenguajes. Y, aunque Visual Studio es la mejor herramienta para trabajar con esta plataforma, también dispone de una serie de herramientas y SDKs (Software Development Kit) para otros sistemas y entornos.

Windows Azure Platform está compuesta de una serie de servicios, los cuales permiten que:

- Los desarrolladores de software creen aplicaciones cloud haciendo uso de sus conocimientos, habilidades y herramientas conocidas.

- Los ISVs y las empresas integradoras de sistemas puedan acceder al mercado con rapidez.

- Los administradores de las Tecnologías de la Información (IT) tengan acceso a un conjunto de nuevos recursos, sin aumentar la complejidad de acceso y uso de estos.

- Todas las empresas (independientemente de su tamaño) puedan responder con agilidad y rapidez a medida que cambian las necesidades comerciales o de demanda.

Los servicios que componen Windows Azure Platform son los siguientes:

- Windows Azure: Es el Sistema Operativo en la nube de Microsoft, y es donde se apoya Windows Azure Platform. Ofrece a los desarrolladores software servicios de ejecución y almacenamiento bajo demanda. Sustentándose en este Sistema Operativo en la nube, los desarrolladores pueden ejecutar y gestionar sus productos en los centros de datos de Microsoft.

- Windows Azure Platform AppFabric: Es la parte que permite una comunicación segura entre las aplicaciones que se ejecutan en una empresa y las que se ejecutan en la nube (Windows Azure). Esto es posible gracias a que Windows Azure proporciona autorización, autenticación y mensajería para que esto se pueda llevar a cabo.

- Microsoft SQL Azure: Se trata de una base de datos relacional en la nube que permite realizar consultas desde cualquier lugar y en cualquier momento. Es como un servidor de datos SQL acondicionado para funcionar en la nube, lo que hace que la disponibilidad sea una prioridad. Es importante remarcar que Microsoft SQL Azure es el primer gestor cloud que puede realizar y entender consultas en SQL.

- AppFabric Service Bus: Proporciona a los desarrolladores la opción y la flexibilidad para elegir cómo se comunican sus aplicaciones.

- AppFabric Access Control: El servicio de control de acceso facilita la generación de una autorización federada entre aplicaciones y servicios sin las complejidades de programación que a veces se necesitan para proteger aplicaciones que traspasan los límites de una empresa u organización.

- Marketplace: Con este servicio los desarrolladores pueden encontrar, obtener y gestionar suscripciones a datos.

6.2.4 Empresas en el mercado español (PaaS)

Vamos a pasar a ver algunos ejemplos de empresas que ofrecen este tipo de servicios dentro del territorio español que, como veremos a continuación, son los menos ofrecidos en España. Algunas de las empresas que dan servicio de la capa Plataforma como Servicio en nuestro país son:

- IBM: El gigante azul ofrece soluciones en todas las capas del Cloud Computing, y es de los pocos que ofrece soluciones en la capa PaaS

dentro del territorio español. Cuenta con un entorno de desarrollo con diversos servicios de aplicación, de ciclo de vida, servicios de integración, y de cargas de trabajo. Las principales características son las siguientes:

- El ciclo de vida de las aplicaciones desarrolladas o que se ejecutan en el entorno de IBM SmartCloud proporciona entornos de desarrollo integrados en la nube, y basados en el trabajo en equipo, que es un punto clave. Proporciona un proceso colaborativo en tiempo real, tanto en desarrollo como en implantación, y cuenta con servicios tales como planificación ágil, gestión del cambio o gestión de la configuración del software. Con todo esto se consigue que el desarrollador se centre en la implementación de los servicios despreocupándose de aspectos como la implantación y la gestión de un entorno donde ejecutar luego dicho servicio.

- Los recursos de las aplicaciones ayudan a reducir costes y complejidad mediante servicios compartidos, es decir, que se dispone de un servicio central y compartido para las necesidades comunes que puedan tener las aplicaciones.

- Los entonos de aplicación facilitan la implantación y la gestión de las aplicaciones: se pueden implantar aplicaciones sin preocuparse por la infraestructura que se tiene y/o se necesita. Se proporciona una escalabilidad y una gestión automatizada a las aplicaciones para múltiples entornos. También se adapta a los distintos tipos de aplicaciones que se puedan tener.

- Con la gestión de aplicaciones con la que cuenta IBM SmartCloud, se pueden implantar aplicaciones y gestionar tareas complejas tales como la gestión del cambio, el back up, la actualización de las aplicaciones, etc.

- Gracias a la integración con la que se cuenta, se sincronizan los datos y procesos en las aplicaciones, es decir, que se pueden sincronizar los datos y procesos de las aplicaciones utilizando un conjunto de conectores de aplicación que son usados por un motor central (y que es configurable) de integración. Así, se consigue una integración de aplicaciones sencilla, sin la necesidad de una codificación concreta ni de la utilización de procesos manuales.

- Oracle: Esta multinacional cuenta con una serie de servicios para la capa Plataforma como Servicio. Cuenta con aplicaciones como *Exadata* y *Exalogic*, software de *Oracle Database*, *Application Grid* y diversos productos para la integración y gestión de procesos en el entorno de Oracle. Todas estas soluciones, junto con las que Oracle proporciona para el resto de capas de la nube, son gestionadas a través de *Oracle Enterprise Manager*, que garantiza una gestión global del entorno cloud.

6.3 Empresas de la capa IaaS

Por último, vamos a ver una serie de empresas centradas en la capa Infraestructure as a Service de Cloud computing que existen hoy en día.

6.3.1 Amazon Web Services

Ilustración 21 - Amazon Web Services [23]

Amazon Web Services es un conjunto de servicios de computación a distancia denominados servicios Web (Web services) que proporciona Amazon.com, y que forman parte de una plataforma Cloud Computing. Su lanzamiento se produjo en Julio de 2002, y después han ido añadiendo servicios y productos a lo largo de los años.

Amazon Web Services ofrecen un grandísimo catálogo de servicios que se clasifican en varios grupos. Los más importantes son: Procesamiento de datos, almacenamiento, redes, entrega de contenido, bases de datos y mensajería. Además, tiene otros servicios que se engloban en los grupos: Pagos y facturas, despliegue y gestión, soporte, tráfico Web y personal.

A continuación se explican los distintos servicios que se ofrecen en cada grupo.

6.3.1.1 Servicios de Procesamiento de datos.

La lista de productos que se ofrecen en esta sección son los siguientes:

- Amazon Elastic Compute Cloud (EC2): Es uno de los servicios más destacados de Amazon Web Services. Consiste en un servicio Web que proporciona capacidad informática y está expresamente diseñado para facilitar a los desarrolladores recursos informáticos escalables y basados en la Web pagando solo por lo que se utilice en cada momento. Además, cuenta con una interfaz de servicios Web que proporciona un control sobre los recursos informáticos. También disminuye el tiempo que se necesita para obtener y arrancar nuevas instancias de servidores, lo cual posibilita el poder aumentar o reducir la capacidad en cualquier momento, dependiendo de las necesidades que se tengan en cada situación.

  Viendo un poco más de detalle, EC2 cuenta con un entorno informático virtual que facilita utilizar interfaces de servicio Web con el fin de crear instancias con distintos sistemas operativos, cargarlas con un entorno de aplicaciones propio, mantener y gestionar los permisos de acceso a la red y ejecutar dicha imagen sirviéndose de los sistemas que el usuario desee.

- Amazon Elastic MapReduce: También denominado EMR, se trata de un servicio Web que permite procesar inmensas cantidades de datos de forma provechosa.

  Se puede usar para momentos en los que se necesite realizar tareas que contengan un elevado uso de datos en aplicaciones, tales como extracción o almacenamiento de datos, análisis financiero, análisis de archivos de registro, etc. Así, el usuario se podrá centrar en el análisis de esos datos.

- Auto Scaling: Este servicio permite escalar de forma automática la capacidad de Amazon EC2, para aumentarla o disminuirla según las

condiciones que se definan. Así, se aumentarán de forma automática las instancias de Amazon EC2 en momento en los que haya picos de demanda, y se reducirán cuando esos picos terminen. Es especialmente útil para aplicaciones que tienen un mayor uso en horas determinadas o fechas determinadas. Está disponible a través de Amazon CloudWatch (servicio del grupo de Despliegue y gestión que veremos más adelante).

- Elastic Load Balancing: Es un servicio que se encarga de distribuir el tráfico entrante de las aplicaciones entre varias instancias de Amazon EC2. Consigue un aumento en la tolerancia a fallos en sus aplicaciones ya que se cuenta con la capacidad de equilibrio de carga necesaria y de respuesta al tráfico entrante de aplicaciones. Detecta instancias que estén en mal estado dentro de un conjunto, y redirige el tráfico hacia las instancias que estén en buen estado hasta que se arreglan las instancias que estaban mal.

6.3.1.2 Servicios de Almacenamiento de datos

Los servicios de almacenamiento que tiene Amazon Web Services son los siguientes:

- Amazon Simple Storage Service (S3): Este es otro de los productos más conocidos dentro de los servicios ofrecidos por Amazon Web Services. Se trata de un servicio de almacenamiento en Internet. A través de una simple interfaz de servicios, el usuario puede almacenar y recuperar cualquier tipo de información cuando quiera y desde donde quiera. Con ello los desarrolladores tienen acceso a una infraestructura económica, muy escalable, fiable, segura y rápida, y que es la misma infraestructura

que utiliza Amazon para mantener en funcionamiento su red mundial de sitios Web. La finalidad de este producto es maximizar las ventajas del escalado y trasladar esas ventajas a los desarrolladores y usuarios finales. Algunas de las funcionalidades que tiene Amazon S3 son las siguientes:

- Se pueden crear, visualizar o eliminar elementos de hasta 5 terabytes.
- Cada objeto se almacena en un depósito, y se recupera por medio de una clave exclusiva asignada por el desarrollador.
- Los depósitos se almacenan en Regiones. Se ha de elegir una Región cercana para minimizar latencia, costes y afrontar exigencias reguladoras.
- Se disponen de mecanismos de autenticación para garantizar su seguridad frente a accesos no autorizados.
- Es flexible y permite añadir de forma sencilla protocolos y/o capas funcionales.
- Los datos almacenados son seguros, ya que solo los propietarios de los objetos y depósitos tienen acceso a esos recursos que ellos crean.
- …

- Amazon Elastic Block Store (EBS): Este producto proporciona volúmenes de almacenamiento a nivel de bloque creados y diseñados para utilizarlos con instancias de Amazon Elastic Compute Cloud (EC2). Estos volúmenes que facilita EBS constituyen almacenamiento fuera de las instancias de EC2 y perduran más allá de la vida de una instancia. Así, tienen una alta disponibilidad y fiabilidad, y se pueden adjuntar a una instancia de Amazon EC2 en ejecución. Este servicio puede resultar muy útil para aplicaciones o servicios que requieren una base de datos, un sistema de archivos o un acceso a almacenamiento a nivel de bloque.

- AWS Import/Export: Es un servicio con el que se pueden realizar transferencias de grandes cantidades de datos tanto hacia Amazon Web Services como desde AWS. De esta manera, AWS extrae de (en caso de transferir desde dispositivo a AWS) o transfiere sus datos a (cuando se transfiere desde AWS a un terminal) dispositivos de almacenamiento utilizando la red interna de alta velocidad de Amazon, sin tener que utilizar Internet, ya que suele resultar más rápido y rentable que realizarlo a través de Internet.

6.3.1.3 Servicios de Redes

Los productos que se ofrece AWS de Redes son los siguientes:

- Amazon Route 53: Se trata de un servicio Web DNS (sistema de nombres de dominio), que ofrece a desarrolladores y a entidades una forma fiable y rentable de direccionar los usuarios finales a las aplicaciones en Internet. Eso se hace transformando los nombres legibles para las personas (como por ejemplo: www.uc3m.es) en direcciones IP numéricas (como 192.168.1.1), que es lo que utilizan los sistemas para conectarse entre ellos. Así, Route 53 conecta de manera eficaz las solicitudes de usuario con las infraestructuras que se están ejecutando en Amazon Web Services.

- Amazon Virtual Private Cloud (Amazon VPC): Con este producto se tiene la posibilidad de tener una sección privada y aislada de la nube de Amazon Web Services en la que se pueden lanzar recursos de AWS en la red virtual que defina el desarrollador. Se puede definir una topología de

red virtual que sea igual o prácticamente la misma que la topología que utilice en el centro de datos de la entidad. Además, el desarrollador tiene el control total sobre el entorno de red virtual, como la elección del rango de direcciones IP, la creación de subredes, etc.

- AWS Direct Connect: Este servicio posibilita el establecimiento de una conexión de red dedicada desde las aplicaciones de Amazon Web Services. Con este producto se puede establecer una conexión privada entre AWS y el centro de datos o entorno de una empresa, que en muchos casos puede repercutir en reducción de costes de red, aumento del rendimiento de ancho de banda y suministro de una experiencia de red más coherente que las conexiones basadas en Internet.

6.3.1.4 Servicios de Entrega de contenido

En este apartado de entrega de servicio hay un servicio ofrecido por AWS, y es el siguiente:

- Amazon CloudFront: Es un servicio Web que consiste en la entrega de contenido. Se integra con otros servicios de AWS, y ofrece tanto a los desarrolladores como a las entidades una forma fácil de distribuir contenido a usuarios finales con unas características: altas velocidades de transferencia, baja latencia y sin compromiso. Además, admite la entrega de contenido dinámico, es decir, partes del sitio Web que cambian para cada usuario final.

6.3.1.5 Servicios de Bases de Datos

El conjunto de productos ofrecidos dentro del grupo de Bases de datos son los que se enumeran a continuación:

- Amazon SimpleDB: Este servicio se encuentra en versión beta (prueba). Se trata de un almacén de datos no relacionales de alta flexibilidad y disponibilidad que libera parte del trabajo de administración de bases de datos. Así, los desarrolladores solo tienen que almacenar los datos y consultarlos cuando necesiten mediante solicitudes de servicios Web, de todo lo demás se encarga Amazon SimpleDB (crea y gestiona varias réplicas de los datos del desarrollador, y los distribuye geográficamente para tener elevada flexibilidad, disponibilidad y capacidad de duración).

- Amazon Relational Database Service (Amazon RDS): Este servicio también se encuentra en versión beta (a fecha 19 de junio de 2012), y facilita las tareas de configuración, utilización y escalado de una base de datos relacional basada en la nube. También ofrece una capacidad rentable y de tamaño variable, y a su vez, gestiona las tareas de administración de la base de datos, lo que permite al desarrollador centrarse en su cometido y negocio.

- Amazon ElastiCache: Al igual que los otros dos servicios ofrecidos de este grupo, se encuentra en fases de prueba (beta). Este servicio Web ayuda a la implementación, funcionamiento y escalado de una memoria caché en memoria en la nube. Mejora el rendimiento de las aplicaciones Web, facilitando la recuperación de información de un sistema de almacenamiento de caché en memoria rápido y gestionado. De esta manera, Amazon ElastiCache simplifica y descarga la gestión,

supervisión y el funcionamiento de los entornos de caché en memoria, lo que permite centrarse en las distintas aplicaciones.

6.3.1.6 Servicios de Mensajería

Las aplicaciones de mensajería que ofrece Amazon Web Services son las siguientes:

- Amazon Simple Queue Service (SQS): Es un sistema con el que los desarrolladores pueden transferir datos entre componentes de aplicaciones que realizan distintas tareas sin perder mensajes. Esto es posible ya que Amazon SQS ofrece un sistema de gestión de colas de mensajes fiable y ampliable para almacenar dichos mensajes a medida que van de unos sistemas a otros.

- Amazon Simple Notification Service (Amazon SNS): Este producto se encuentra en fase de pruebas (beta). Se trata de un servicio Web con el que se pueden configurar, utilizar y enviar notificaciones desde la nube de Amazon. Ofrece a los desarrolladores capacidad escalable, flexible y rentable para publicar mensajes desde una aplicación y entregarlos de forma inmediata a suscriptores o a otras aplicaciones. De esta forma y a través de una interfaz de servicios Web y una consola, se pueden crear temas sobre temas de los que se quiere informar (a aplicaciones o personas), se pueden suscribir clientes a estos temas (para que reciban todos los mensajes que se den de alta de ese tema) y para que esos mensajes se entreguen a través del protocolo que se elija (e-mail, sms, etc.).

- Amazon Simple Email Service (Amazon SES): Al igual que el servicio anterior, este también se encuentra en versión beta. Este es un servicio de envío de correo electrónico masivo y transaccional económico y muy ampliable según la necesidad, dirigido a desarrolladores y empresas. Con este servicio se cambia el paradigma, ya que no es necesario el gasto en la construcción de una solución de correo electrónico, licencias, uso de un servicio de otro proveedor, etc. Además, Amazon SES está integrado dentro de otros servicios de AWS, lo cual facilita el envío de aplicaciones alojadas en servicios como Amazon EC2.

6.3.1.7 Servicios de Pagos y facturación

Los servicios de este grupo son los siguientes:

- Amazon Flexible Payments Service (FPS): Este servicio es el primer servicio de pagos diseñado desde el principio para desarrolladores. Está construido en lo alto de infraestructura de pagos de Amazon (que tiene una alta fiabilidad y escalabilidad), y proporciona a los desarrolladores una buena vía de cobro a los clientes finales. Eso es así ya que estos clientes pueden pagar usando las mismas credenciales, direcciones de envío e información de pago que ya tienen en los archivos de Amazon.
  Con Amazon FPS los desarrolladores pueden realizar operaciones tales como aceptar pagos en su sitio Web por la venta de bienes o servicios, ejecutar pagos recurrentes, enviar pagos, etc. Además, les ofrece una gran flexibilidad en la forma de estructurar las instrucciones de pago.

- Amazon DevPay: Es un servicio de facturación online y administrador de cuentas que facilita a los negocios el vender aplicaciones que están

desarrolladas o alojadas dentro de Amazon Web Services. Es un servicio diseñado para facilitar a los desarrolladores que las aplicaciones se ejecuten en la nube bajo demanda. Con este servicio se elimina la complicación por parte de las entidades de tener que crear y administrar su propio sistema de facturación.

6.3.1.8 Servicios de Despliegue y gestión

A continuación se detallan los servicios ofrecidos dentro de este grupo de despliegue y gestión para la capa Infraestructura como Servicio:

- AWS Identity and Access Management (IAM): Con este servicio se puede controlar de forma segura el acceso a los diferentes servicios y recursos de Amazon Web Services por parte de los usuarios. Esto es así ya que Amazon IAM permite crear y administrar usuarios en AWS y otorgar acceso a los recursos de AWS a los usuarios que se gestionan. Además, ofrece gran seguridad, flexibilidad y control al utilizar AWS.

- Amazon CloudWatch: Facilita la supervisión de los recursos de la nube de Amazon y de las aplicaciones que ejecutan los clientes en Amazon Web Services. Supervisa recursos de AWS tales como las instancias de bases de datos de Amazon EC2 y Amazon RDS (vistos con anterioridad), y también tiene la opción de supervisar métricas personalizadas generadas por las aplicaciones y servicios de un cliente concreto. De esta manera, Amazon CloudWatch proporciona una visibilidad para todo el sistema de la utilización de los recursos, rendimiento de las aplicaciones y el estado del funcionamiento.

- AWS CloudFormation: Este producto ofrece tanto a desarrolladores como administradores de sistemas un sistema fácil para crear y ofrecer colecciones de recursos de AWS, a partir de plantillas de muestra de AWS CloudFormation, o creando ellos mismos sus propias plantillas que describan los recursos AWS y las posibles dependencias o parámetros de tiempo de ejecución que se necesitan para la ejecución de las aplicaciones.

6.3.1.9 Servicios de Soporte

En este grupo se ofrece un único servicio:

- AWS Support: Es un canal de soporte de comunicación directa y respuesta rápida que funciona las 24 horas de los 365 días del año, que ofrece apoyo de ingenieros experimentados. Este servicio da soporte a usuarios de todos los tamaños y habilidades técnicas para conseguir la buena y completa utilización de los servicios ofrecidos por Amazon Web Services. Todos los niveles de apoyo que conforman Amazon Support ofrecen a los clientes de los servicios de infraestructura AWS un número ilimitado de casos de ayuda. Consta de cuatro niveles, que proporcionan tanto a entidades como a desarrolladores la flexibilidad para elegir los niveles de ayuda que respondan sus necesidades específicas.

6.3.1.10 Servicios de Tráfico Web y Personal

Los servicios que se engloban en estos dos últimos grupos que analizamos no son propiamente de la capa Infraestructura como Servicio (IaaS), por lo que damos una breve descripción de ellos sin entrar en detalles:

- Alexa Web Information Service: Facilita a los desarrolladores los datos con los que cuenta Alexa (empresa subsidiaria de Amazon que provee información acerca de la cantidad de visitas que recibe un sitio Web, clasificando los resultados en un ranking), que contiene datos sobre patrones de tráfico y estructuras de la Web.

- Alexa Top Sites: Proporciona datos sobre tráfico de sitios Web a nivel internacional, ya que dispone de un sistema que recopila y actualiza de forma continua los datos.

- Amazon Mechanical Turk: Permite a las empresas el acceso a miles de trabajadores mundiales bajo demanda.

6.3.2 GoGrid

Ilustración 22 – GoGrid [24]

GoGrid es una empresa estadounidense dedicada a proveer servicios de la capa Infraestructura como Servicio de Cloud Computing. Es decir, que la entidad GoGrid está especializada en ofrecer soluciones de infraestructura en la nube.

Su primera plataforma de Cloud Computing (y una de las primeras del mercado) se lanzó en Marzo de 2008. Desde entonces y hasta ahora, ha conseguido ofrecer a sus clientes una de las soluciones en la nube más flexibles, robustas, de más alto rendimiento y basada en estándares.

GoGrid está compuesto por una serie de componentes de infraestructura. A continuación se detallan cada uno de ellos:

- Servidores en la nube: Los servidores Cloud de GoGrid están preconfigurados de tal manera que permite a los clientes finales ponerlos en marcha en muy poco tiempo. A su vez, los clientes tienen las siguientes facilidades: tienen control total sobre las imágenes que tengan ,con permisos root (de administrador), tienen la posibilidad de agregar datos y aplicaciones a los servidores y tienen el control sobre la localización del centro de datos. En el área de desarrollo, los desarrolladores pueden elegir dentro de una gran variedad de opciones.

- Servidores dedicados: Se trata de potentes servidores físicos que son administrados directamente a través del portal de GoGrid. Estos servidores son ideales para ejecutar aplicaciones para las que el cliente no quiera que posea un entorno de multi-tenencia, como por ejemplo bases de datos que requieran el cumplimiento PCI (que son las siglas de *Payment Card Industry Compliance*, es decir, las normas desarrolladas para proteger los datos de los propietarios que realizan un pago).

- Balanceadores de carga: Son balanceadores de carga de F5 (compañía estadounidense dedicada a aplicaciones de red para entidades). Estos balanceadores están incluidos en todas las cuentas de GoGrid, y su configuración se hace de forma simple y rápida. Se contemplan dos casos de uso: prevenir tiempos de inactividad de la aplicación (para que cuando se difunde el tráfico de Internet a través de dos o más servidores, en el caso de que un servidor no esté disponible ser redirija el tráfico a los servidores activos) y rápida escalabilidad y tiempo de actividad (para cuando aplicaciones Web sufren un incremento repentino de tráfico, que los balanceadores escalen la infraestructura para las necesidades del momento).

- Almacenamiento en la nube: En la nube de GoGrid se ofrece un servicio escalable y fiable de backup para servidores cloud de Windows y Linux que se ejecutan en la nube de GoGrid. Estos servidores montan su volumen de almacenamiento a través de una red privada, y hacen uso de protocolos comunes para mover los datos dentro o fuera de la nube de almacenamiento. Solo se paga por el volumen de almacenamiento que se usa, pudiendo mantener controlado lo que se gasta.

Aparte de los componentes y productos que componen GoGrid, tiene una serie de características principales, que se resumen a continuación:

- Múltiples centro de datos: Con las herramientas de las que dispone GoGrid se pueden desplegar las infraestructuras en cualquiera de los centros de datos de los que dispone GoGrid. Esto facilita a las empresas establecer infraestructuras en puntos geográficos diferentes, manteniendo un único proveedor de Infraestructura como Servicio.

- Imágenes de servidores en la nube personalizables: Esto significa que se pueden crear, guardar, compartir e implementar imágenes de servidores en la nube de GoGrid.

- API de código abierto: Permite a los desarrolladores controlar su interacción con la infraestructura de alojamiento en la nube de GoGrid. Proporciona comunicación en la programación para administrar la infraestructura en la nube del desarrollador.

- Exchange de GoGrid: El Exchange de GoGrid permite compartir o vender imágenes de servidores de GoGrid a su comunidad.

- RAM escalable en la nube bajo demanda: GoGrid ofrece una escalabilidad fácil y rápida de los servidores en la nube. De forma sencilla se puede aumentar y disminuir la memoria RAM de un servidor de la nube según se necesite en cada momento.

- Aplicación para iPhone: Cuenta con una aplicación para iPhone con la que un cliente puede administrar su infraestructura en la nube desde su terminal.

6.3.3 Empresas en el mercado español (IaaS)

En este subapartado vamos a definir brevemente ejemplos de empresas que ofrecen servicios de la capa Infraestructura como Servicio, ya porque sean empresas españolas, o porque aunque no sean españolas, ofrezcan estos servicios en nuestro país.

La lista de empresas se detalla a continuación:

- 1&1: Es una entidad de hosting que ofrece servidor en la nube dinámico tanto con Windows como con Linux. Con esto, el cliente puede adaptar la configuración del servidor, el número de CPUs, la memoria RAM y el tamaño de disco duro en función de las necesidades del negocio. Además, cuenta con acceso root y tráfico ilimitado. Adicionalmente, cuenta con una aplicación para Android y iPhone con la que se puede gestionar el servidor desde cualquier parte.

- VMware: Es de los fabricantes más importantes de soluciones de virtualización para centro de datos y escritorio. Con la última versión de la plataforma líder en virtualización, *VMware vSphere 5*, ofrece importantes mejoras de escalabilidad y rendimiento, y funcionalidades de gestión que ayudan a cualquier entidad u organización a crear las bases para el desarrollo de infraestructuras en la nube. Así, VMware permite a las empresas meterse en el Cloud Computing mejorando la gestión, el control y la seguridad del centro de datos.
  Además, este año 2012 VMware lanzará *Project Octopus* en versión beta, que proporcionará a las organizaciones almacenamiento cloud, ofreciendo a los usuarios una manera fácil, rápida y segura de compartir información desde cualquier lugar y dispositivo, tanto a nivel interno como externo de la entidad.

- Acens: Se trata de una compañía de hosting que en 2011 fue comprada por Telefónica. Cuenta con una plataforma muy robusta que da soluciones bajo nubes privadas, públicas, híbridas o sitios Web flexibles. El cliente puede elegir diferentes opciones que satisfagan sus necesidades, soluciones que contienen integración de numerosas

tecnologías tanto a nivel hardware como software, tecnologías de las que dependen la seguridad, disponibilidad y rendimiento de la plataforma.

- Altimate: Es un mayorista especializado en el mercado de la seguridad que tiene una asociación con Oracle desde principios de 2011. Su principal oferta de servicios se basa en Exadata Database Machine, una solución para el aumento exponencial de la velocidad de los procesos que ofrece un rendimiento muy elevado para el almacenamiento de datos y procesamiento de transacciones online.
  Además, en el área de almacenamiento en la nube cuenta con una serie de propuestas, sobre las que destaca Oracle Cloud Computing. La finalidad de Altimate es ofrecer buenas y fiables soluciones que permiten aumentar la capacidad de almacenamiento de las organizaciones, facilitando almacenamientos compartidos en grupo con espacios de nombres unificados para aplicaciones, archivos de usuarios y archivos operativos.

- Arsys: Esta compañía localizada en Logroño ofrece una serie de soluciones de IaaS:
  - *CloudBuilder*, servicio que permite gestionar centros de datos virtuales con total flexibilidad, disponibilidad y versatilidad (tanto en nube pública, hibrida y privada), pagando solo por lo que se usa.
  - *CloudPC*, con la que se pueden virtualizar puestos de trabajo y alojar en la nube los ordenadores corporativos. CloudStorage es una solución para empresas que necesitan gran capacidad de almacenamiento para guardar información a bajo coste.
  - *DiscoDuroOnline* es un servicio para profesionales y PYMES (pequeñas y medianas empresas) con capacidad ilimitada,

escalabilidad automática hasta 1 TeraByte, permisos de usuario y total disponibilidad y seguridad.

- *BackUp Online*, servicio con el que se pueden hacer copias de seguridad de forma remota para PYMES y profesionales.

- APC: Es una empresa fabricante de SAIs (Sistemas de alimentación ininterrumpida). Empresas como APC dedicadas a la fabricación de SAIs tienen un papel importante en la nube ya que en estos nuevos entornos la protección y la seguridad ante posibles eventualidades y anomalías relacionadas con la disponibilidad de energía es algo esencial. Por esto, APC ofrece una arquitectura denominada InfraStruxure que permite seleccionar componentes estandarizados mediante configuraciones modulares y móviles en infraestructuras físicas de redes críticas que integran potencia, refrigeración, gestión y servicios. De este modo se logra una arquitectura escalable que permitirá cubrir las necesidades que requiera el negocio en cada momento. Este producto está disponible desde para armarios de cableado hasta para grandes centros de datos.

- Bcnbinary: Esta empresa con sede en Barcelona ofrece servicios de la capa IaaS para pequeñas y medianas empresas. Entre los servicios que ofrece están la virtualización de escritorios (*Escritorio Virtual*) o recursos compartidos (*beCloud*). Algún caso de éxito puede ser el Servicio de Sistemas y Comunicaciones de la Consejería de Sanidad de la Generalitat Valenciana.

- Eaton: También se trata de un fabricante de SAIs. Su solución se basa en el uso de sistemas energéticos modulares escalables que nunca sufren una pérdida energética y se pueden ampliar según las necesidades. Con esto, la familia de productos de la marca, *Eaton 9x55, BladeUPS 9390 y*

9395, tienen unas características técnicas que permiten mejorar la fiabilidad de sus infraestructuras en la nube, al permitir añadir redundancia a la arquitectura energética y emplear un software de gestión integrado.

- Emerson Network Power: Al igual que APC y Eaton, se trata de un fabricante de SAIs. Su solución se basa en la problemática de que la computación en la nube puede generar grandes problemas si no tiene una infraestructura robusta que garantice la continuidad del servicio en caso de incidencias, averías, etc. Por ello, Emerson Network Power ofrece soluciones como AC Power, equipos de refrigeración y racks, que dinamizan la gestión de infraestructuras y la monitorización. Además de esto, también ofrecen servicios para garantizar la continuidad de forma segura.

- Cisco: Esta empresa fabricante de hardware, se ha definido como proveedor de data center del modelo Cloud Computing gracias a la transformación que ha realizado en su propia compañía. Cisco ayuda a diseñar, implementar y utilizar entornos en la nube a empresas y proveedores mediante la oferta de infraestructura, soluciones y servicios. En infraestructura, Cisco facilita servidores UCS (servidores con sistemas de computación unificada de la propia marca), switches, routers y herramientas de seguridad y movilidad de red.

- Citrix: Es un fabricante de software y una importante empresa dentro del mercado de la virtualización. Aparte de eso, dispone de un equipo hardware para dar soluciones a infraestructuras en la nube:

- *NetScaler Cloud Gateway* reduce de manera importante la disposición y gestión de las aplicaciones y servicios informáticos, y ayuda a los departamentos de IT a reemplazar sus arquitecturas tradicionales a un enfoque basado en servicios.
- *Citrix NetScaler Cloud Bridge* permite conectar de manera transparente data centers corporativos con cualquier nube externa, convirtiendo este último en una extensión de la red empresarial. De esta manera se logra una mayor seguridad y se reducen los costes finales.

- Fujitsu: Empresa fabricante de hardware, Fujitsu terminó en 2011 la construcción de una red mundial de centro de datos, con una alta eficiencia energética y que ofrece altos niveles de protección de datos, fiabilidad de servicio y seguridad. Este servicio está dentro de la plataforma *Global Cloud*, y se llama *Plataforma Global Cloud*. A su vez, ha creado seis centros globales (en Japón, Australia, Singapur, Estados Unidos, Reino Unido y Alemania), donde los usuarios cuentan con la garantía total de que se acogen a la legislación local vigente con la máxima seguridad y privacidad.
  Además, tiene un servicio de almacenamiento en la nube revolucionario. *Eternus DX8700 S2* redefine el almacenamiento flexible bajo tres pautas: capacidad, altas prestaciones y conectividad, que proporcionan a su vez escalabilidad y modularidad multidimensional.

- GTI Software & Networking: Es uno de los principales mayoristas de software del mercado español. Mediante la implantación de nubes públicas que ofrece a sus proveedores, estos pueden desplegar una serie de servicios que ofrecen a sus clientes. GTI también ofrece productos específicos para compañeros del sector que quieren ofrecer servicios en

torno a esa nube, servicios que también son aplicables a empresas de hospedaje o vendedores de software independiente (ISV) que quieran gestionar la infraestructura de sus clientes.

- HP: La apuesta de Hewlett-Packard por la Infraestructura como Servicio viene con *HP CloudSystem*, un entorno que facilita una plataforma para construir y gestionar servicios cloud a través de entornos públicos, híbridos o privados. Los clientes aseguran la fiabilidad, calidad del servicio y la reducción de riesgos gracias a la seguridad universal, el gobierno y la gestión multi-tenencia que caracterizan a este producto.
  Además, HP cuenta con un producto para el almacenamiento en la nube, *HP 3PAR*, que ofrece toda la agilidad que exigen los entornos cloud hoy en día y que permite la virtualización de los centros de datos.

- Mast Storage: Es una compañía española especializada en la fabricación de software. Ofrece soluciones de copia de seguridad para el entorno profesional, como backup a cinta, backup a disco y servicio de copia externalizada (Mast Backup Online). La oferta de Mast Storage está diseñada tanto para pequeñas empresas como para grandes organizaciones con grandes volúmenes de información.

- Ingram Micro: Este mayorista, a través de Areté Sistemas que ya está integrada en el sistema, ha entrado en el negocio de Cloud Computing. Ha realizado una apuesta muy importante por la nube, punto que se demuestra tras la inversión de tres millones de euros que se han destinado a la puesta en marcha de un data center basado en sistemas HP y cuya arquitectura también es una arquitectura de HP.

- Intel: Esta multinacional fabricante de hardware, dentro de su estrategia *Cloud 2015*, apuesta por la nube con los procesadores *Intel Xeon E7* para servidores. Con estos procesadores se consigue acelerar las aplicaciones informáticas críticas, que repercute en que permiten a los departamentos informáticos de las entidades gestionar entornos de grandes volúmenes de datos con mayor eficacia gracias a las nuevas funciones de seguridad, fiabilidad y rendimiento. Además, permite aumentar el rendimiento hasta un 40% respecto a procesadores de gamas anteriores, lo que facilita el proceso de implantación de las infraestructuras como servicio.

- OVH: Se trata de una empresa proveedora de servicios que ha aterrizado en España en los últimos tiempos. A través de su nube privada, permite a las entidades crear su propia infraestructura en la nube en muy poco tiempo. Así, en unos cuantos *clicks* el cliente concibe su data center o centro de datos, para después poder desarrollar y desplegar sus máquinas virtuales. Cabe comentar que todos estos elementos están integrados y configurados a su interfaz de gestión, que no es otra que *vSphere* de *VMware* (visto con anterioridad). La nube privada de OVH es una solución dedicada: tiene una serie de recursos reservados para el único uso del cliente y cada uno de los equipamientos es doble (servidores, red, espacios de almacenamiento, etc.).

- Strato: Proveedor de servicios con más de cinco años de experiencia en el mercado español, tiene una serie de ofertas para profesionales, autónomos y PYMES que quieran alojarse en Internet a un coste asequible. También ofrece paquetes completos de alojamiento Web con múltiples funcionalidades y servicios en la nube, como *Strato HiDrive* (almacenamiento online) o *Strato Comunicator* (correo webmail).

- Telefónica: La operadora adquirió Acens (proveedor de servicios con una gran cuota de mercado), lo que le dio más capacidad para entrar en el negocio de la nube. Ofrece una serie de servicios:

    - *Virtual Data Center*, servicio con el que los clientes cuentan con un data center completo que se puede gestionar a través de un portal de forma fácil e intuitiva.
    - *PC Virtual*, con el que el ordenador de un usuario deja de residir en una máquina física para alojarse en la nube.
    - *Cloudphone*, que permite a los usuarios tener en un único dispositivo móvil el teléfono personal y profesional.

- Oracle: Este fabricante provee todo tipo de componentes tecnológicos, hardware y software para permitir prestar servicios IaaS a clientes finales y proveedores de servicios. Entre estos componentes se incluye una completa propuesta de almacenamiento que es capaz de: garantizar la eficiencia en la gestión gracias a la provisión del almacenamiento de manera rápida y eficiente; garantizar la calidad del servicio gracias a que *Oracle Pillar Axiom 600* permite asignar recursos en función de la criticidad de las aplicaciones y además cambiar estas prioridades de forma temporal y permanente si es necesario; garantizar una escalabilidad lineal, puesto que los sistemas Oracle tienen una arquitectura modular que permite empezar solo con lo necesario para después ir creciendo sin cambios en la base.

  Además, otras soluciones que ofrece para la capa Infraestructura como Servicio son servidores, hardware de red, tecnologías de virtualización y sistemas operativos.

- Aparte de las empresas mencionadas anteriormente, hay una serie de servicios orientados a usuarios finales más que a organizaciones y corporaciones para el almacenamiento y alojamiento de información en la nube. Los más famosos en la actualidad son Dropbox, Google Drive o Windows Skydrive. Cada uno de ellos ofrece una capacidad de almacenamiento gratuita para cada usuario, que luego se puede aumentar pagando un "alquiler".

- Otras empresas que ofrecen servicios de la capa Infraestructura como Servicio dentro del mercado español son las siguientes: Afina, AMD, Dell, IBM, Informática El Corte Inglés, Iomega, Magirus, Microsoft, Riello Enerdata, Socomec o Vodafone.

Capítulo 7:

Control en Cloud Computing

7.Control en Cloud Computing

En este punto, lo primero que vamos a ver es la legislación aplicable al Cloud computing. Dentro de la legislación vamos a ver la regulación de la Ley Orgánica de Protección de Datos, la Regulación de la Ley de Servicios de la Sociedad de Información y la Regulación del Código Penal.

En otro apartado vamos a ver los distintos riesgos y amenazas que existen, que se engloban en 3 subapartados: riesgos de infraestructura, riesgos técnicos y riesgos legales y contractuales.

7.1 Legislación

Como hemos ido viendo a lo largo de este documento, las principales características del Cloud Computing son la de ofrecer servicios a través de Internet para que el usuario los utilice como si los tuviera en su propia organización o equipo (en local), y la de gestionar de forma remota todos los datos de los clientes que tenga el propio proveedor de la nube.

Esta información que las entidades y usuarios finales transfieren a los distribuidores de la nube puede ser a veces sensible, ya que pueden alojarse en servidores ubicados en otro país que no sea España o que tenga un marco jurídico de protección de datos distinto al español. Esto acarrearía una serie de condicionantes que se deberían tener en cuenta conforme a lo que se establece en el marco normativo nacional de protección de datos de carácter personal.

Como se menciona anteriormente e iremos viendo a continuación más en detalle, este tipo de situaciones acarrean una serie de implicaciones jurídicas ya que, en el caso de que la información de un usuario esté alojada en un país diferente al país de origen de este, se dará el caso en el que haya que evaluar dos jurisdicciones (en el presente documento se tendrá a España como el país origen de los datos de los usuarios u organizaciones).

Cuando convergen dos jurisdicciones hay que decidir multitud de aspectos como la Ley aplicable en cada caso, las condiciones que se han de exigir para asegurar una transferencia segura de los datos del cliente al proveedor y en tal caso sea autorizada por la autoridad pertinente de protección de datos del usuario (en nuestro caso España), etc.

Finalmente se firma el contrato con sus términos de uso, con lo que tanto el proveedor como el usuario se comprometen a aceptar la jurisdicción especificada en el documento.

Cabe mencionar que España cuenta con un marco jurídico riguroso que ampara normativamente el desarrollo del mercado del cloud computing. El marco diseñado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre (RDLOPD), marcan las condiciones básicas a cumplirse y que regulan la seguridad y la protección de los datos de carácter personal necesarias para poder considerar a España como un entorno jurídico seguro para el desarrollo y despliegue del Cloud Computing.

El contexto normativo a tener en cuenta se cita y desarrolla en los subapartados siguientes.

7.1.1 Regulación de la LOPD

Antes de comenzar este punto vamos a pasar a definir una serie de conceptos y entidades:

- LOPD: Estas siglas corresponden a la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**. Tiene por objeto garantizar y proteger, en lo concerniente a los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

- RDLOPD: **Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal**.

- AEPD: Son las siglas correspondientes a la **Agencia Española de Protección de Datos**. Su objetivo es garantizar el cumplimiento de este tipo de normativa dentro del territorio Español.

Con estas definiciones claras podemos pasar a hablar de la regulación de la LOPD.

Como dice la definición, LOPD es la Ley de Protección de Datos de Carácter Personal, por lo que lo primero que debemos hacer es tener en cuenta cómo define dato personal la LOPD en su artículo número 3:

> *"Artículo 3. Definiciones.*
>
> *A los efectos de la presente Ley Orgánica se entenderá por:*
>
> ***a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.***
>
> *b) ...*
>
> *c) ..."*

Con esta definición que la LOPD da de dato personal nos encontramos dos escenarios excluyentes. El primero es que los datos con los que se trabaje en la nube pertenezcan a este grupo, y el segundo es que los datos que manejemos en la nube no pertenezcan a este grupo:

- En el caso de que los datos que se vayan a manejar en la nube pertenezcan a esta clase, la empresa que trate estos datos debe asegurarse previamente a su tratamiento que cumple con la totalidad de las obligaciones que se describen en la LOPD, como que asegure la calidad y protección de los datos, que cumplan el deber de secreto, que se garanticen los derechos de acceso, rectificación, cancelación y oposición, etc.

- El segundo escenario es si los datos que se vayan a manejar en la nube no pertenecen a la categoría especificada. Si es así, se podrán realizar las tareas, operaciones, etc. de esos datos sin impedimento de la LOPD.

Otro de los puntos clave a la hora de tratar datos personales en Cloud Computing es cuando en la prestación de servicios, el responsable contrata a su vez servicios a un tercer implicado, ajeno a esta. Este escenario es la

denominada **prestación de servicios por terceros ajenos al responsable**. La LOPD y el RDLOPD denominan a este tipo de prestación de servicios un encargo del tratamiento.

La definición que el RDLOPD da al encargo del tratamiento en su artículo 5 es la siguiente:

> *"Artículo 5. Definiciones.*
>
> *1. A los efectos previstos en este reglamento, se entenderá por:*
>
> *a) ...*
>
> *...*
>
> ***i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.***
>
> *j) ...*
>
> *..."*

Con lo visto hasta ahora en este punto, a continuación se detallan, por un lado los artículos y títulos de la LOPD y del RDLOPD concernientes a la seguridad de los datos, y por otro los artículos de la LOPD y del RDLOPD relativos al acceso de los datos por parte de terceros.

<u>Artículos referentes a la seguridad de los datos:</u>

- Artículo 9 de la LOPD

"Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

- Título VIII del RDLOPD

"TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo

dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:
a) Los relativos a la comisión de infracciones administrativas o penales.
b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.
c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:
a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten

redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:
a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultarle aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. Encargado del tratamiento.

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las

medidas de seguridad previstas en el citado documento. Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán

garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Una posible implantación de este Artículo 85 en la computación en la nube podría ser la utilización de cifrado a la hora de acceder a ese tipo de datos de carácter personal a través de redes de comunicaciones. Esta medida de seguridad sería imprescindible (o una similar) si esos datos estuvieran catalogados con un alto nivel alto de seguridad, como pueden ser la salud. De esta manera se conseguiría un nivel de seguridad equivalente al que se tiene en local, que es lo que se exige en este Artículo 85.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:
a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

SECCIÓN 1.ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Una posible implantación del Artículo 94 sería realizar lo siguiente:

Un posible camino para la realización de copias de seguridad se podría hacer mediante backups, el cual, si durante la semana hubiera algún cambio en los datos se activaría, se realizaría el backup de manera inmediata, y de no haber ningún cambio, no se activaría y no se realizaría el backup. De esta manera se puede optimizar el procedimiento de copias de respaldo, pudiendo

utilizar dichos recursos en otros ámbitos de la computación en la nube.

Para reaccionar ante posibles pérdidas, en caso de fallo, el procedimiento que podría haber debería activar la última imagen de backup de los datos que se hubiera hecho. En caso de que la pérdida afecte a ficheros o datos parcialmente automatizados, podría existir un procedimiento que en caso de fallo grabe la situación previa al error, para después poder grabar manualmente esos datos y poder evaluar el motivo del defecto. De esta manera se podría anticipar a posibles fallos en el futuro y, así, evitar errores similares una vez se han producido en la nube.

SECCIÓN 2.ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la

adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

La implantación del Artículo 99 puede tener alguna dificultad, debido a que en la nube puede pasar que los equipos físicos que dan soporte a los sistemas que utiliza un cliente estén en un país diferente de donde se encuentran dichos clientes y donde desempeñan su actividad.
Por ello, en caso de que el cliente quiera saber el estado de estos equipos, una posible solución a este problema podría ser mandar un listado con los puntos que el cliente quiere que se verifiquen, para que las personas (empleados del proveedor de servicios Cloud) que se encuentran en el lugar donde se encuentran los equipos informáticos puedan verificarlos, para después enviarle el listado con sus correspondientes anotaciones. También es posible que como respuesta se envíe un informe de auditores, ya sea internos o externos.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

SECCIÓN 3.ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Para llevar a cabo la implantación de este Artículo número 102, las copias de respaldo de nivel alto podrían guardarse en centro de datos de la nube que se encuentren en un país distinto a donde se encuentren dichos datos, en otra ciudad, o incluso en un lugar ignífugo de otro edificio que no se vea afectado por las mismas amenazas que pueda tener el sitio físico donde se encuentran los equipos. En el caso de que se encuentren en un país distinto al que originalmente se encuentran los equipos informáticos, cabe mencionar que ese país donde se guardara esa copia de seguridad debería tener el mismo nivel de seguridad que el país original donde se encuentran los datos, ya que de otra manera no se podría conservar dicha copia de seguridad en ese país.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales. La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Como se ha propuesto en el Artículo 85, una posible implantación de esas medidas de seguridad podría ser el cifrado de los datos. En este Artículo 104 menciona que el cifrado de

datos se debería realizar cuando el nivel de seguridad de los datos sea alto. No obstante, para evitar que se pierda la confidencialidad e integridad de información, y que por consecuencia se puedan perder, sería recomendable el cifrado de todo tipo de datos cuando se realicen transmisión de datos a través de redes públicas o redes inalámbricas de comunicaciones. De esta manera aseguraríamos la seguridad de todo tipo de datos.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

SECCIÓN 1.ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:
a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

SECCIÓN 2.ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

SECCIÓN 3.ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado."

Cabe mencionar que los artículos de este último Capítulo (Capítulo IV del Título VIII del RDLOPD) relacionado con las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados no son estrictamente aplicables a procesos relacionados con la computación en la nube.

Artículos referentes al acceso de los datos por parte de terceros:

- Artículo 12 de la LOPD

"Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente."

- Artículo 20 del RDLOPD

"Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo. El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido. No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este
Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo."

- Artículo 21 del RDLOPD

"Artículo 21. Posibilidad de subcontratación de los servicios.

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:
a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior. En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior."

- Artículo 22 del RDLOPD

"Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso

> *deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.*
>
> *2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento."*

Estos artículos y títulos pertenecientes tanto a la LOPD como al RDLOPD, reúnen toda la serie de puntos que se tienen que tener en cuenta sobre la seguridad de los datos y el acceso de esos datos por terceras personas a la hora de firmar las cláusulas de un contrato.

Referente a los artículos 9 y 12 de la LOPD, la mayoría de contrataciones se realizan bajo condiciones generales (excepto en casos muy particulares) establecidas para un conjunto general de clientes, donde además se pueden añadir políticas de privacidad. Por esta razón, es muy importante que el cliente se asegure de que el proveedor de servicios cloud se compromete a cumplir, respetar y velar por las obligaciones establecidas en los artículos mencionados (relativos a la seguridad de los datos y el acceso a los datos por parte de terceros).

Otro de los aspectos a tener en cuanta es cuando los datos ubicados en la nube pertenecientes a una empresa se encuentran en países diferentes al propio país de esta. En nuestro caso, cuando los datos de una empresa o cliente español están ubicados fuera del territorio español o del Espacio Económico Europeo (que comenzó su existencia el 1 de enero de 1994 con motivo de un acuerdo entre países miembros de la Unión Europea y de la Asociación Europea de

Libre Comercio). A esta situación se le denomina transferencia internacional de datos, cuya definición es la siguiente:

- Transferencia internacional de datos: Es el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

La transferencia internacional de datos obliga a discernir entre los países que forman parte del Espacio Económico Europeo y terceros países ajenos a este grupo. Si la transferencia de información se da entre estados pertenecientes al EEE, se siguen las reglas ordinarias sobre el encargado del tratamiento. En cambio, si el traspaso de datos se realiza entre países ajenos a este grupo, se tendrán que tener en cuenta algunos artículos de la LOPD y del RDLOPD.

A continuación se detallan los artículos tanto de la LOPD como del RDLOPD que regulan este tipo de situaciones:

Artículos de la LOPD:

- Título V de la LOPD:

"TÍTULO V

Movimiento internacional de datos

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido

recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado."

Artículos del RDLOPD:

- Título VI del RDLOPD:

"TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. Cumplimiento de las disposiciones de la Ley

Orgánica 15/1999, de 13 de diciembre. La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. Autorización y notificación.

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento. La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:
a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.
b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un

determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior. Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. Nivel adecuado de protección declarado por Decisión de la Comisión Europea.

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. Suspensión temporal de las transferencias.

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:
a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.
b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente

reglamento. En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos. La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:
a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento. Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento. En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español. En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento."

Estos artículos de la LOPD y del RDLOPD regulan la transferencia internacional de datos. Pero pueden existir situaciones en las que no se den los escenarios adecuados que cumplan lo descrito en estos artículos. Cuando esto ocurra, se deberá seguir el procedimiento siguiente, descrito en el RDLOPD:

- Sección 1ª del Capítulo V del Título IX del RDLOPD:

"CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

SECCIÓN 1.ª PROCEDIMIENTO DE AUTORIZACIÓN DE TRANSFERENCIAS INTERNACIONALES DE DATOS

Artículo 137. Iniciación del procedimiento.

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:
a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.
b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso. Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes. Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. Instrucción del procedimiento.

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde

la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. Actos posteriores a la resolución.

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción. El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos."

Siguiendo este procedimiento especificado en el RDLOPD, se obtendrá la autorización del Director de la AEPD, y entonces se podrán realizar transferencias internacional de datos.

La lista de países integrantes del Espacio Económico Europeo es la siguiente: Austria, Bélgica, Bulgaria, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Irlanda, Italia, Liechtenstein, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Noruega, Polonia, Portugal, Rumania, Eslovaquia, Eslovenia, Suecia, Reino Unido y España.

Además, la lista de países cuyo nivel de protección se considera equiparable al Espacio Económico Europeo por la AEPD que se establecen según el Artículo 67, dentro del Capítulo II del Título VI del RDLOPD son los siguientes:

- **Suiza**, de acuerdo con la Decisión de la Comisión 2000/518/ CE, de 26 de julio de 2000.

- Las **entidades estadounidenses adheridas a los principios de "Puerto Seguro"** (safe harbor), de acuerdo con la Decisión 2000/520/CE de la Comisión de 26 de julio de 2000. Safe harbor son los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos.

- **Canadá** respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos, de acuerdo con la Decisión 2002/2/CE de la Comisión de 20 de diciembre de 2001.

- **Argentina**, de acuerdo con la Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003.

- **Guernsey**, de acuerdo con la Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.

- **Isla de Man**, de acuerdo con la Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.

- **Jersey**, de acuerdo con la Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.

- **Islas Feroe**, de acuerdo con la Decisión 2010/146/UE de la Comisión de 5 de marzo de 2010.

- **Andorra**, de acuerdo con la Decisión 2010/625/UE, de la Comisión de 19 de octubre de 2010.

- **Israel**, de acuerdo con la Decisión de la Comisión de 31 de enero de 2011 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

- **Uruguay**, que se ha añadido a esta lista recientemente. Desde el 21/08/2012 se considera un país con nivel de protección equiparable por la Unión Europea. De acuerdo con el Artículo 25, apartado 2, de la Directiva 95/46/CE, se garantiza que cumple un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea. Lo dictamina la Decisión 2012/484/UE de Ejecución de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que

respecta al tratamiento automatizado de datos personales y extensiva a todo el EEE.

7.1.2 Regulación de la LSSI

En primer lugar vamos a definir lo que significan las siglas LSSI:

- LSSI: Se trata de las iniciales de la Ley de Servicios de la Sociedad de la Información de España, aunque su nombre completo es **Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico**.

Sabiendo lo que significan las siglas LSSI, podemos decir que la totalidad de proveedores de servicios tales como servicios de acceso a Internet o como lo que nos ocupa, los servicios relacionados con el Cloud Computing, han de estar controlados y han de cumplir todas las obligaciones y requisitos que se establecen en la LSSI.

Más concretamente, el conjunto de proveedores de servicios ubicados en España tienen la obligación de mantener informados a sus clientes de manera constante, gratuita y directa sobre los siguientes temas:

- Las medidas técnicas que aplica el proveedor de servicios para aumentar la seguridad de la información que se maneja. Así, el usuario sabrá en todo momento las técnicas utilizadas por el distribuidor de servicios, con lo que podrá estar más tranquilo sabiendo que su información no corre peligro.

- Las medidas de seguridad que el proveedor establece para la provisión de los servicios que ofrece a los clientes.

- Ante la posibilidad de que los servicios puedan ser utilizados por menores o por otro tipo de público (por ejemplo, una empresa que no quiera que sus empleados accedan a ciertos recursos o páginas en Internet), ha de incluir las herramientas necesarias para filtrar y restringir el acceso a los contenidos y servicios no deseados o que puedan resultar nocivos o perjudiciales.

- Los proveedores de acceso a Internet han de comunicar de manera directa a los usuarios las responsabilidades que podrían tener el hacer un mal uso o un uso ilícito de la red del proveedor de servicios. De esta manera, si un usuario utiliza dichos servicios para realizar actividades ilegales, en caso de ser descubierto podrán tomarse medidas legales contra ese usuario.

Además de todo esto, la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico especifica las obligaciones y responsabilidades que tienen las empresas según las actividades que realicen. Algunas de las actividades que se reflejan con sus correspondientes obligaciones y responsabilidades son: realizar comercio electrónico, hacer publicidad por vía electrónica, empresas que prestan servicios de intermediación de la Sociedad de la información, para usuarios de Internet que sean titulares de páginas personales, etc.

7.1.3 Regulación del Código penal

En este punto nos encontramos ante una situación bastante compleja, puesto que los entornos en la nube pueden llegar a tener un gran número de cuestiones a plantear. Esto es así ya que las características del Cloud Computing como la transferencia de datos y procesos a terceros, la deslocalización de la información (características vistas con anterioridad en este punto), etc. pueden incitar a posibles ciberdelincuentes a cometer actos delictivos.

En la mayoría de los casos estos actos delictivos tienen que ver con la estafa, mediante la creación de sitios Web falsos en la nube para hacerse con información de distintos usuarios, mediante la distribución de software maligno para posteriormente realizar ataques de fraude en la red, etc.

Por todo esto, la estafa se regula en el Código Penal en el artículo 248, que fue revisado y reformado en 2010 según la Ley Orgánica 5/2010, de 22 de junio. La reforma del artículo 248 del Código Penal dice lo siguiente:

> *"Se modifica el artículo 248, que queda redactado como sigue:*
>
> *«1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.*
>
> *2. También se consideran reos de estafa:*
> *a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.*
> *b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.*

> *c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.»"*

Otro de los puntos que más relación puede tener el Cloud Computing con el Código Penal es la revelación de secretos. Se puede producir un robo de información personal o secreta por varios motivos. Un caso de robo podría ser la información que ciertos usuarios pueden llegar a apropiarse aprovechándose de debilidades o fallos de seguridad en algunos sistemas de la información. Otra situación podría ser gracias a las habilidades que estos delincuentes tienen para pasar desapercibidos (invisibles) para posteriormente hacerse con información de usuarios.

A continuación se expone el Artículo 197 del Código Penal, perteneciente al Título X y Capítulo I del descubrimiento y revelación de secretos. Cabe mencionar que el artículo que se especifica a continuación viene actualizado con las modificaciones que se han hecho en las siguientes leyes: Ley Orgánica 5/2010, de 22 de junio; Ley Orgánica 3/2011, de 28 de enero.

El artículo 197 del Código Penal es el siguiente:

> *"Artículo 197.*
>
> *1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b a g del apartado 7 del artículo 33.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

7. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el

apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado."

7.2 Riesgos de la utilización de entornos en nube

El Cloud Computing, como todas las tecnologías que existen, tiene una serie de riesgos y amenazas asociados. En este caso, al tratarse de una tecnología muy joven y en constante crecimiento, hace que tenga mayor número de riesgos (algunos probablemente aún desconocidos) que los expertos en seguridad tratan de paliar o eliminar día a día.

A continuación se pasan a describir las principales amenazas existentes en Cloud Computing.

7.2.1 Riesgos de Infraestructura

Las amenazas de infraestructura que existen son las que se detallan en los subapartardos siguientes.

7.2.1.1 Abuso y mala utilización del Cloud Computing

La nube ofrece un gran número de facilidades y oportunidades, y como es normal, esas facilidades están también al alcance de usuarios que no tienen como finalidad algo positivo. Este tipo de amenazas suelen afectar principalmente a los servicios ofrecidos en las capas PaaS e IaaS.

Así, cualquier usuario que pague los servicios en la nube (con una tarjeta de crédito/débito, por ejemplo) puede acceder a los servicios ofrecidos por el proveedor Cloud, con el correspondiente riesgo a que utilicen esos servicios para realizar ataques como el robo de contraseñas, envío de spam, creación de código malicioso, etc. Incluso hay criminales que utilizan la nube como centro de operaciones para llevar a cabo su objetivo.

Una de las ventajas que están de parte de los delincuentes es que en el caso de realizar un ataque o un acto delictivo a través de la nube, cuando terminan de realizarlo, los recursos que han utilizado para llevarlo a cabo se borran, lo que dificulta mucho el seguimiento y persecución por parte de la policía. De la misma manera, si algún ciberdelincuente se dedica a almacenar en la nube datos o información robados o de procedencia ilegal, será difícil acceder a dicha información ya que no se sabe dónde se encuentran los datos en la nube en cada momento.

Algunos pasos que se pueden seguir para intentar evitar este tipo de comportamiento son:

- Hacer un seguimiento del fraude por tarjetas de crédito/débito

- Monitorizar el tráfico y actividad de los clientes para detectar un posible comportamiento ilegal.

- Tener un sistema de registro de accesos más restrictivo.

- Realizar una comprobación de las listas negras públicas (listas de dominio público para evitar, por ejemplo, el spam) para comprobar si los rangos IP de la infraestructura cloud han entrado en ellas.

7.2.1.2 Amenaza interna

Este tipo de riesgos están presentes en todos los sistemas de información, y los entornos en la nube no iban a ser menos.

Los propios usuarios de una empresa, entidad u organización, al tener acceso a los datos y a las aplicaciones de forma normal, pueden llegar a ser la amenaza más grande, ya sea porque el empleado cometa un error, porque desconozca el funcionamiento de alguna aplicación, o por el descontento que pueda tener este con la empresa.

Normalmente el proveedor de servicios (en este caso el proveedor de servicios en la nube) es el encargado de gestionar las altas y las bajas de los usuarios que pueden acceder a los servicios. Y es en este punto donde en ocasiones se produce falta de comunicación cuando la entidad consumidora no avisa al proveedor de posibles bajas de personal en la organización.

Al final, este conjunto de incidentes pueden ocasionar grandes pérdidas de imagen, pérdidas económicas y pérdidas de información, por lo que sería recomendable, incluso necesario, que el proveedor de servicios de la nube facilite medios para el seguimiento y localización de estas posibles amenazas.

Algunas recomendaciones que se pueden llevar a cabo para disminuir este tipo de riesgos son:

- Especificar cláusulas legales y de confidencialidad en los contratos laborales (que se hace normalmente)

- Establecer políticas de seguridad para evitar posibles fugas de información.

- Como se ha mencionado, que el proveedor del servicio facilite métodos para la localización de estas amenazas internas.

- Realizar hojas de seguimiento de los empleados, reflejando tareas realizadas, nivel de satisfacción, etc.

7.2.1.3 Pérdida de información importante

Este punto es similar al anterior, pero solo como la posibilidad de perder información importante para la entidad, no por medio de un empleado descontento o insatisfecho.

Al igual que en los distintos sistemas de información en el Cloud Computing se puede perder información debido a un borrado o modificación sin haber realizado previamente una copia de seguridad.

Como en el punto anterior, este tipo de pérdidas de información pueden conllevar pérdidas económicas y de imagen para la organización. Y de tratarse de fugas de información puede llegar a haber problemas legales.

Estas pérdidas de información pueden ser debidas, por ejemplo, al resultado de una auditoría débil, al mal uso de las claves de cifrado, etc.

Algunas recomendaciones en este punto son:

- Proteger la trasferencia de datos e información mediante el cifrado de todo el contenido a enviar.

- Contar con fuertes mecanismos para la generación de claves, para el almacenamiento de estas y de la información, y para la destrucción de la información en caso de que fuera necesario.

- Realizar un análisis de los datos en tiempo de ejecución de forma periódica.

- Definir una buena política a la hora de realizar copias de seguridad de la información que se posee.

- Implementar APIs potentes para el control de acceso (ver punto siguiente).

7.2.1.4 APIs e Interfaces inseguras

Las APIs e Interfaces son el único punto de conexión con las aplicaciones que se ejecutan en la nube. Dicho de otra forma, son las puertas de entrada a través de las cuales podemos acceder a los servicios que ofrece el proveedor cloud y gestionar los recursos que tiene. Al ser esto así, estas herramientas se convierten en un punto crítico a la hora de mantener la seguridad y privacidad del sistema, ya que mantienen el control, la provisión y la monitorización de los servicios cloud.

Es importante mencionar que cada proveedor de servicios en la nube tiene sus propias Interfaces y APIs para acceder a las servicios que ofrece, por lo que no es algo general para todos los proveedores, sino que cada uno de ellos tendrá que tener una fuerte política de seguridad para evitar ataques que puedan derribar esa puerta de entrada, con las terribles consecuencias que podría tener.

Algunas de las consecuencias derivadas del ataque a las Interfaces y APIs de un proveedor cloud pueden ser permitir el acceso anónimo, tener una autenticación sin cifrar, limitaciones a la hora de gestionar los logs... todo ello con el fin de acceder a la información, robarla, modificarla, etc.

Existen algunas recomendaciones para evitar sufrir este tipo de ataques:

- Analizar los problemas de seguridad tanto en las Interfaces como en las APIs de los proveedores del servicio para su posterior fortalecimiento.

- Asegurar que se realiza el cifrado de datos a la hora de realizar la autenticación y los controles de acceso.

7.2.1.5 Suplantación de identidad

Este riesgo no es solo un problema del Cloud Computing, sino de todos los sistemas informáticos. Sin embargo, en los entornos en nube tiene especial relevancia.

Casi la totalidad de sistemas informáticos piden identificación antes de poder realizar las tareas que se necesite llevar a cabo. Y normalmente esa identificación se realiza por medio de un usuario y una contraseña.

En el caso de que un atacante obtenga dichas credenciales de un usuario, tendrá acceso al sistema, a las tareas, datos, información, etc. con el correspondiente riesgo a que manipule la información o envíe información falsa a clientes o compañeros.

Si fortalecemos esa identificación usando, por ejemplo, el DNI electrónico, sería más complicado por parte del atacante el secuestro de la sesión del usuario, ya que el DNI electrónico incluye medidas biométricas y criptográficas aparte de la identificación tradicional de usuario y contraseña.

Otras recomendaciones para ayudar a prevenir este tipo de riesgos son:

- Monitorizar las sesiones de los usuarios en busca de actividades inusuales.

- Aplicar técnicas de autenticación más potentes (como el DNI electrónico explicado arriba).

- Prohibir a través de políticas la compartición de credenciales.

7.2.1.6 Problemas derivados del Hardware compartido

Este tipo de problemas están relacionados con los servicios ofrecidos por la capa IaaS del Cloud Computing. Existen algunos componentes hardware como CPUs o unidades de procesamiento gráfico (GPUs), cuyo diseño no está pensado para una arquitectura de compartición de aplicaciones.

Para evitar incidentes relacionados con este tipo de problemas, se recomienda la implementación de técnicas y métodos de defensa que se centren especialmente en los recursos de red, de computación y de almacenamiento. En adición, también es recomendable tener una buena estrategia de seguridad que se encargue de gestionar los recursos, de manera que las tareas que realiza un usuario no provoquen problemas en el resto de funciones desarrolladas por los demás consumidores.

A continuación se describen algunas recomendaciones para evitar estos problemas derivados del hardware compartido:

- Realizar buenos diseños para la instalación y configuración de la infraestructura.

- Tener un fuerte control de acceso y autenticación para el acceso a la administración de recursos.

- Monitorización de los entornos activos para detectar posibles cambios no deseados en la actividad o configuraciones de los mismos.

- Mantener un control de los niveles de servicio para la corrección de posibles vulnerabilidades.

7.2.1.7 Planes inadecuados frente a desastres

Es posible que en un momento dado la empresa proveedora de servicios en la nube sufra algún tipo de desastre, ya sean naturales o externos como un terremoto, desastres como inundaciones o incendios, averías en equipos y comunicaciones, o por algún tipo de virus.

Este tipo de situaciones pueden llegar a provocar daños a personas, equipos, instalaciones, etc. También pueden tener como consecuencia pérdidas económicas, que ofrezcan un peor servicio o pérdida de imagen de la propia empresa. Y para el usuario podría conllevar la pérdida total o parcial de la información que almacenaba, de los procesos que estaba ejecutando, etc.

Para hacer frente a este tipo de situaciones que pueden darse en cualquier momento es necesario contar con un buen plan de Continuidad del negocio así como un buen plan de recuperación frente a desastres. Con estos planes, la vuelta a la normalidad sería rápida y eficiente, con lo que las pérdidas descritas anteriormente se podrían disminuir en gran medida y el usuario podría volver a ejecutar las tareas que necesitase con total normalidad.

En caso de no contar con un plan de contingencia y recuperación frente a desastres, las consecuencias podrían llegar a ser devastadoras, incluso podría

conllevar el fin de la actividad del negocio del proveedor y a la pérdida de la información y tareas que el usuario estaba alojando en la nube.

Algunas recomendaciones para evitar esto son:

- Que el proveedor cuente con un buen plan frente a desastres, que garantice la continuidad e integridad de la información del cliente.

- Que el proveedor disponga de un plan de Continuidad del negocio frente a las situaciones descritas a continuación.

- Que se tengan copias de seguridad de la información de los clientes en otros lugares aparte del lugar original, para que en caso de desastre, la información de los clientes no se vea afectada.

7.2.1.8 Desconocimiento del perfil de riesgo

En todos los entornos informáticos la seguridad ha sido y es un tema tan importante como estudiado.

A la hora de hablar del Cloud Computing la seguridad implica un nuevo cambio no conocido hasta el momento. Las nuevas funcionalidades, servicios y el crecimiento de las oportunidades que tiene la nube, hace que también crezcan los riesgos y amenazas. Al contrario de lo que pueda parecer, no es que se trate de un sistema menos seguro que los anteriores, sino que al ser un modelo joven y en continuo crecimiento, aún hay multitud de amenazas por descubrir, experiencia que se irá adquiriendo con el tiempo.

De esta tarea se encargan los expertos en seguridad, que investigan para descubrir la forma de actuar de los usuarios malintencionados además de tratar de mejorar posibles fallos del diseño. Uno de los temas clave es el uso de tecnologías compartidas y el aislamiento imprescindible de la información de usuarios que comparten una misma infraestructura.

Por otra parte, el Cloud Computing tiene uno de sus pilares en reducir en gran medida el software y hardware que tiene que adquirir la entidad, para alquilarlo a los proveedores de la nube. Es un gran punto de diferenciación, pero es importante que este ahorro en software y hardware no conlleve un deterioro en la seguridad por falta de conocimiento de la infraestructura que se utiliza.

Para evitar esta falta de seguridad es muy recomendable saber, al menos de forma parcial, la información técnica de la infraestructura sobre la que vamos a ejecutar nuestro sistema, datos, información, etc. El no tener este tipo de información, puede tener graves consecuencias como brechas de seguridad que sean desconocidas por el afectado.

Una serie de recomendaciones para este tipo de riesgos por desconocimiento son:

- Estar al corriente, de forma parcial o total, de los detalles de la infraestructura, como por ejemplo con quién se comparte, los intentos de acceso no autorizados, etc.

- Tener acceso a los registros de actividad (logs) de aplicaciones y datos.

- Monitorizar y recibir información sobre el uso de información crítica para la entidad.

- Informarse y verificar las políticas de seguridad que tiene el proveedor cloud, si tiene equipo de investigación para nuevas posibles amenazas, etc.

7.2.2 Riesgos técnicos

En este apartado se van a describir los riesgos presentes desde el punto de vista técnico, es decir, los que se pueden dar en el proceso de acciones que realiza el proveedor cloud.

7.2.2.1 Compartición de recursos

Esta amenaza existe ya que los sistemas e infraestructuras de un proveedor de la nube pueden estar siendo utilizados por varios clientes finales. En un momento dado se podría dar la situación de que ciertos usuarios accedan a información que no les pertenece, lo que sería una grave fuga de seguridad por parte del proveedor del servicio.

Por esto, existen una serie de recomendaciones para evitar que este tipo de situaciones lleguen a darse:

- La implantación de fuertes controles de seguridad que se encarguen de que cada usuario solo pueda acceder a su información, es decir, que de ningún modo puedan acceder a información ajena.

- En adición a la recomendación anterior, en los sistemas que puedan ser compartidos por varios clientes, instalar barreras de seguridad alrededor del rango e información de cada usuario, para dar un plus de seguridad a la hora de mantener la privacidad de los datos.

7.2.2.2 Abuso de privilegios

Los administradores del proveedor cloud tienen todos los privilegios sobre los servicios que ofrecen. De esta manera, en cualquier momento estos administradores pueden acceder a información confidencial de empresas, clientes, usuarios, etc.

Este tipo de abuso es hacer un uso ilícito de las funciones que puede hacer un administrador de sistemas, aparte de que sobrepasa las funciones que debe hacer.

Por todo ello, a continuación se dan una serie de consejos para evitar y/o detectar este tipo de comportamiento:

- Monitorización de las acciones que realizan los administradores del servicio en todo momento, por las acciones que puedan realizar.

- Sistema de alertas que avise en caso de que algún superusuario haga abuso de los derechos que le han sido asignados.

- Realizar un adecuado otorgamiento de permisos de administrador, ya que contribuirá en un mejor funcionamiento y uso de la nube.

- Controles periódicos para verificar si en algún momento algún administrador del servicio ha realizado funciones que sobrepasan sus obligaciones.

7.2.2.3 Dimensionamiento inadecuado de recursos asignados

El proveedor cloud debe realizar un buen cálculo de los recursos que deben ser asignados a cada cliente por dos razones: para que el cliente tenga los recursos que necesita en cada momento, y para que el proveedor no haga una mala asignación de recursos que repercuta en un derroche de recursos innecesario.

Si un usuario accede a la nube y no tiene los recursos necesarios, esto puede tener consecuencias negativas tanto para el cliente (que no podrá realizar las tareas que tenía programadas) como para el proveedor (que puede perder clientes debido al descontento de estos).

Así, existen unas advertencias para evitar que esto ocurra:

- Realizar un cálculo de los recursos que necesita una entidad o cliente de forma permanente, para que en ningún momento el usuario tenga que dejar de realizar las acciones que desea realizar. Así, si se presenta un

momento en el que se tiene un pico de trabajo, el usuario debe comunicárselo al proveedor para que este haga lo propio haciendo un redimensionamiento adecuado de los recursos asignados a ese cliente.

7.2.2.4 Comunicaciones inseguras entre cliente y proveedor

Como ya se sabe, la comunicación entre el proveedor de Cloud Computing y el cliente final se hace siempre a través de Internet. Y esto es un riesgo puesto que en Internet hay multitud de ciberdelincuentes que pueden poner en riesgo la información que mandamos, que recibimos, etc.

Para evitar ataques en la comunicación entre el usuario final y el proveedor de la nube se puede realizar lo siguiente:

- Mantener una buena y robusta política de cifrado de la información a la hora de mandarla de cliente a proveedor y viceversa. Así se evitan posibles acciones ilícitas por parte de usuarios de Internet malintencionados.

- Utilizar un canal de transferencia de información seguro a través de Internet. Esto también ayudará a evitar posibles ataques a la información que se maneja.

7.2.2.5 Eliminación de la información

Existen situaciones en las que los datos de un cliente deben ser eliminados por diversos motivos (legales, término de una relación contractual, etc.). Pero no siempre la eliminación se hace de forma completa.

Hay situaciones en las que los archivos solo son parcialmente eliminados, lo que resulta insuficiente ya que se deben borrar de forma íntegra.

Para evitar que la eliminación de los datos se quede a la mitad o que no se haga de forma completa, es recomendable seguir estos consejos:

- Asegurar, mediante la firma de contratos, la eliminación de toda la información al término de la relación contractual, o por los motivos que se especifiquen en el contrato. También se puede realizar un bloqueo de los datos personales para atender a posibles responsabilidades futuras o consultas que se pudieran realizar, de manera que esta información no pueda ser accedida salvo emergencia.

- Incluir en los contratos los certificados de borrado o destrucción que utiliza el proveedor de la nube para la eliminación de la información.

7.2.2.6 Denegación de servicio

Las empresas que ofrecen servicios a través de Internet, entre las que están incluidas todas aquellas que ofrecen servicios Cloud Computing, suelen sufrir una serie de ataques externos, que pueden tener como consecuencia la denegación de servicio (también llamado *DoS* del inglés *Denial of Service*).

La denegación de servicio provoca que los usuarios no puedan acceder al sistema y a los servicios que ofrecen. Esto puede tener graves consecuencias en el caso de que una empresa o usuario tenga que realizar unas tareas críticas y, al no poder acceder al servicio en la nube, no pueda realizarlas.

Para ayudar a evitar estos ataques que dejen sin servicio a los proveedores de la nube se puede realizar lo siguiente:

- Que la propia empresa de Cloud Computing realice un análisis de denegación de servicio, para posteriormente recoger los resultados obtenidos, y con ellos tomar una serie de decisiones para calibrar, minimizar o anular este tipo de ataques en la organización.

7.2.2.7 Insolvencia del proveedor Cloud

Se pueden dar situaciones en las que el proveedor de servicios en la nube sea insolvente. En estas circunstancias la solución suele ser que el centro de datos se pase a otro proveedor. Lo que en principio parece no ser un problema puede generar graves problemas de privacidad, puesto que este tipo de cambios pueden provocar que haya un acceso no restringido por parte de otros usuarios.

Una serie de valoraciones al respecto pueden ser:

- Hacer una valoración de los proveedores cloud que existen, para evitar comenzar una relación contractual con un proveedor que pueda tener problemas económicos.

- Reflejar en los contratos estas situaciones que se pueden llegar a dar, para garantizar al cliente que sus datos e información nunca estarán en peligro.

7.2.3 Riesgos legales y contractuales.

A la hora de clasificar y evaluar este tipo de riesgos es necesario que exista un marco de actuación entre el proveedor de servicios cloud y el cliente que utilizará esos servicios. Este marco de actuación debe enumerar y definir puntos tales como las responsabilidades de las partes, las penalizaciones que pueden darse en caso de que una de las dos partes incumpla el contrato, cómo serán tratados los datos e información, etc.

Las principales amenazas legales y contractuales que se pueden dar se definen en los subapartados siguientes.

7.2.3.1 Deslocalización de la información

Aunque los clientes de la nube la mayor parte de las veces no saben dónde está alojada su información, datos, etc. el proveedor de servicios ha de saber perfectamente en cada momento la ubicación de esos datos. Y en el caso de los datos personales, su ubicación debe conocerlas el cliente.

Así, la entidad contratante sabrá siempre dónde se encuentran los datos e información de todos sus clientes.

7.2.3.2 Protección de datos

Las dos partes que conforman la relación contractual (la entidad contratante o proveedor cloud y el cliente) deben suscribir un contrato, que dependerá de lo siguiente:

- Si el proveedor de servicios en la nube se encuentra en España o se trata de un país con un nivel de protección de datos equiparable al que hay en nuestro país, entonces el contrato deberá ser redactado conforme al artículo 12 de la LOPD**.**

- De no ser así, el contrato redactado deberá estar en armonía con las cláusulas adoptadas en la Decisión 2010/87/UE de la Comisión, del 5 de febrero de 2010.

Independientemente de cualquiera de los dos casos de los que estemos hablando, las medidas y niveles de seguridad que el proveedor de la nube deberá aplicar son las del Título VIII del RDLOPD.

En caso de incumplimiento, las sanciones administrativas establecidas por la normativa de protección de datos pueden llegar hasta los 600.000 Euros.

7.2.3.3 Dependencia del proveedor

Cuando una organización contrata los servicios de un proveedor cloud puede ocurrir que pasado un tiempo esta entidad comience nuevas relaciones con otra

empresa o quiera empezarlas, lo que conllevaría un intercambio de información, y donde se necesitaría una cooperación para la integración y prestación de posibles servicios conjuntos. Esto puede llegar a ser un problema, ya que también puede ocurrir que se de la situación en que una entidad quiera migrar sus servicios a otro proveedor con mejores características.

Por todo ello, es necesario que todas estas cuestiones y posibles situaciones queden reflejadas en el contrato. Además, en caso de no cumplirse alguno de estos puntos marcados en el contrato, pueden llegar a haber sanciones y penalizaciones al no satisfacer las obligaciones de interoperabilidad reflejadas en dicho contrato.

7.2.3.4 Titularidad de los derechos

Todas las creaciones, aplicaciones, desarrollos, información, etc. relativos a la propiedad intelectual y a las que tenga acceso el proveedor de servicios deben quedar reguladas y especificadas en el contrato para evitar posibles luchas y malentendidos en el futuro.

Así, si un cliente, utilizando aplicaciones alojadas en la nube, resulta que llega a la creación de algo nuevo que sea susceptible de ser protegido en materia de propiedad intelectual, deberá estar incluido en el contrato el régimen de titularidad de las creaciones intelectuales que se realicen en la nube.

7.2.3.5 Notificación frente a incidentes graves de seguridad

Como es normal, el proveedor de la nube es el encargado de mantener y gestionar la seguridad de su infraestructura y de los servicios que ofrece.

Existen ocasiones en las que se da un acceso no autorizado, hay un ataque de un pirata informático, y pilares como el centro de procesado de datos, la información de los clientes, etc. se ve expuesta. Todo este tipo de amenazas pueden hacer que disminuya en gran medida la calidad del servicio que se ofrece.

Por ello, el proveedor, además de tratar y solucionar este tipo de sucesos con la mayor rapidez y eficiencia posible, ha de notificar a sus clientes con la mayor celeridad que se ha producido un ataque de estas características, para que el usuario decida en cada caso qué hacer y qué medidas aplicar en caso de que lo crean necesario.

7.2.3.6 No disponibilidad del servicio por parte del proveedor

En el Cloud Computing es fundamental que los clientes puedan acceder a los servicios y a su información en la nube cuando lo necesiten. De no ser así, la imagen del proveedor y la productividad de los clientes y empresas de este se pueden ver afectadas de manera importante.

Para evitar estos momentos de inactividad es necesario definir de forma concreta los tiempos de inactividad permisibles y las pérdidas de información aceptables para el proveedor. Esto se hace mediante un Acuerdo de Nivel de Servicio o ANS, que es un contrato entre el proveedor y el cliente donde se fija el nivel de calidad del servicio en puntos como los descritos anteriormente. En

adición, también puede contemplar medidas compensatorias en caso de incumplimiento de este contrato.

7.2.3.7 Incumplimiento de algún otro tipo de directrices

En Cloud Computing, al igual que en el resto de sistemas, se han de cumplir todas las exigencias, obligaciones y demandas legales especificadas en el contrato.

Todo punto, situación, etc. cuya funcionalidad o presencia se quiera asegurar, se ha de contemplar por escrito en el contrato para obligar a su cumplimiento, y en caso de no satisfacerse, tener por escrito las sanciones y penalizaciones correspondientes que se deberán aplicar.
A continuación se muestra un cuadro resumen con los riesgos vistos en este apartado:

RIESGOS		
Riesgos de Infraestructura	**Riesgos Técnicos**	**Riesgos Legales y Contractuales**
• **Abuso y mala utilización del Cloud Computing.** • **Amenaza interna** • **Pérdida de información importante.** • **APIs e Interfaces inseguras.**	• **Compartición de recursos.** • **Abuso de privilegios.** • **Dimensionamiento inadecuado de recursos asignados.** • **Comunicaciones inseguras entre cliente y proveedor.**	• **Deslocalización de la información.** • **Protección de datos.** • **Dependencia del proveedor.** • **Titularidad de los derechos.** • **Notificación frente a incidentes graves de**

• **Suplantación de identidad.** • **Problemas derivados del Hardware compartido.** • **Planes inadecuados frente a desastres.** • **Desconocimiento del perfil de riesgo.**	• **Eliminación de la información.** • **Denegación de servicio.** • **Insolvencia del proveedor Cloud.**	**seguridad.** • **No disponibilidad del servicio por parte del proveedor.** • **Incumplimiento de algún otro tipo de directrices.**

Tabla 2 - Riesgos Cloud Computing

Capítulo 8:

Guía de migración a la nube

8.Guía de migración a la nube

En este último punto vamos a ver los distintos pasos que tienen que dar los clientes u organizaciones que quieran pasarse a la nube.

Con todo lo visto a lo largo de este documento, ya sabemos todo lo que hay que saber sobre el Cloud Computing para decidir si se quiere o no pasarse a este nuevo modelo. Ya sabemos cómo funciona, las posibilidades que ofrece, qué tipos de nubes existen, los modelos de despliegue que hay, la legislación aplicable, etc.

Así, lo que debemos hacer es seguir los puntos siguientes para saber todo lo que se tiene que ir haciendo, y las decisiones que se han de ir tomando con la finalidad de ver si al cliente realmente se puede beneficiar de todas las posibilidades que da el mundo en la nube.

8.1 Análisis de la situación de cliente

El primer paso a la hora de pasarse a la nube es que la propia entidad que quiere dar el paso a la nube evalúe y verifique una serie de puntos acerca de su actividad, niveles de seguridad a cumplir, etc.

A continuación se detallan estos puntos (por temática) que ha de evaluar cada cliente que quiera pasarse a la nube:

- En cuanto a la actividad que desempeña la empresa, los aspectos a tener en cuenta son los siguientes:

    - Se deben evaluar las áreas del negocio que pueden ser susceptibles de pasar a la nube. Es posible que se quiera migrar una sola área como puede ser contabilidad, el centro de datos, o recursos humanos, hasta la totalidad de su negocio. Por esto, se han de verificar las áreas del negocio que se pueden llegar a migrar a la nube, es decir, las regiones áreas funcionales cuya migración sea factible.

    - Otro aspecto que necesita ser evaluado desde el punto de vista de la actividad que desarrolla la organización es el conjunto de usuarios, empleados, etc. que se van a beneficiar de pasar del modelo que se tiene actualmente a la migración al modelo en la nube. En este punto no solo se han de tener en cuenta los empleados de una empresa que van a su lugar de trabajo asiduamente, sino también los usuarios y empleados que realizan de manera habitual su cometido desde un lugar que no es la propia ubicación física de la empresa (como pueden ser usuarios cuyo trabajo conlleve viajar, como comerciales). Las necesidades y requisitos de este tipo de usuarios han de ser tenidos en cuenta a la hora de pasarse a la nube, para que su trabajo futuro no se vea afectado.

    - Uno de los aspectos más importantes de este grupo es el presupuesto que se tiene y que se gasta en el modelo que actualmente se tiene en la entidad (antes de pasarse a la nube), ya que la finalidad primera de una empresa es tener beneficios, por

lo que cuanto menos gasto en los medios que se utilizan para llegar a los objetivos, más eficiente será todo.

Este aspecto se refiere a los gastos asociados al centro de datos o a las licencias de las aplicaciones que se utilizan. Uno de los puntos fuertes del Cloud Computing es el ahorro que se puede llegar a tener a la hora de utilizar una herramienta en la nube en modo de alquiler en lugar de comprar las licencias como se hacía hasta ahora. De la misma forma, tener el centro de datos (o parte de él) en la nube tiene como consecuencia que el presupuesto que se necesite pueda llegar a ser mucho menor.

- Desde el punto de vista de la seguridad y la tolerancia a fallos, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) estructura en cuatro categorías los parámetros que cada empresa ha de definir para realizar el salto a la nube:

    - La capacidad de la entidad para proporcionar un buen nivel de servicio al mismo tiempo que se asegura la confidencialidad e integridad de la información que se maneja. Esta categoría es la que se encarga de que el nivel de servicio siempre se cumpla, al igual que la seguridad de los datos. Este punto es esencial ya que de no tener un buen nivel de servicio, la actividad de la empresa se vería afectada, y en extensión la empresa en general.

    - Entrega de servicio: Consiste en la capacidad que han de tener los sistemas para proporcionar los servicios de la manera que se ha especificado en el acuerdo de servicio (ANS). Se trata del cumplimiento del contrato firmado.

- Respuesta y recuperación: Se trata de los criterios que se han de tener en cuenta para dar respuesta y recuperarse frente a fallos, averías o incidencias. Dicho de otra forma, se trata de definir los pasos a seguir para volver a la actividad normal de la compañía en caso de que ocurra algún incidente que perjudique el funcionamiento normal de esta.

- Cumplimiento legal y normativo específico de la entidad.

- Se ha de definir el nivel de servicio que se quiere tomar en la Cloud Computing. Como se ha visto a lo largo de este documento, los servicios que ofrece la computación en la nube se agrupan en tres grupos: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS).

- De la misma manera que en el punto anterior, la organización ha de valorar y elegir el tipo de nube donde quieren desplegar los servicios, ya sea una nube pública, una privada, una híbrida o una comunitaria.

Con todos estos aspectos bien presentes, el siguiente paso que debe realizar la empresa que quiere dar el salto a la nube es realizar un análisis DAFO.

8.2 Análisis DAFO

El análisis DAFO, que también es conocido como matriz DAFO, es una herramienta que se encarga de estudiar la situación de una empresa o un proyecto, analizando sus características internas, Debilidades (D) y Fortalezas (F), y su situación externa, Amenazas (A) y Oportunidades (O). De estos cuatro aspectos viene el término DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades).

Esta herramienta es una de las más utilizadas por las empresas para buscar la mejor estrategia a corto, medio y largo plazo. A continuación se muestra un DAFO donde se comparan la situación que hasta ahora había de la compra de licencias, centros de datos en la misma ubicación de la empresa, etc., es decir, del modelo tradicional que se conoce, enfrentado con el nuevo modelo que es el Cloud Computing.

Cabe mencionar que este DAFO se ha construido a partir de un proveedor típico de servicios Cloud Computing.

Análisis DAFO	FORTALEZAS	DEBILIDADES
Análisis Interno	• Ahorro económico debido a que no es necesaria una inversión y mantenimiento por parte del cliente. • Gran oferta de proveedores. • Importante concentración y aumento de la gestión de la seguridad por parte de los proveedores. • Flexibilidad gestionando la variabilidad que puede existir en la demanda en cada momento. • Accesibilidad y movilidad. • El cliente paga por lo que usa en cada momento. • Despliegue de software e infraestructura inmediato. • Apariencia de las aplicaciones, escritorios, etc. en la nube como si estuvieran en local.	• No existen procedimientos específicos para la contratación de servicios Cloud. • Falta de consideraciones previas a la contratación y durante el servicio. • Deslocalización de la información y pérdida de control. • Dependencia del proveedor. • Ingresos vulnerables a fallos de seguridad, disponibilidad, rendimiento, etc. • Entrega a través de Internet (cuya debilidad existe en que si en algún momento falla la conexión, no se puede acceder a los servicios cloud). • Moderada/Fuerte inversión y mantenimiento de la infraestructura.
	OPORTUNIDADES	**AMENAZAS**
Análisis Externo	• Incremento de la estabilidad, ancho de banda, seguridad de Internet. • Compartición de recursos y estandarización común. • Debido a la crisis actual,	• Que exista algún fallo de algún competidor del mercado en cuanto a seguridad, disponibilidad, privacidad, etc. • Ausencia de una normativa específica que regule el modelo Cloud

	las empresas buscan ahorro en costes. • Mercado en crecimiento constante. • A favor de los proveedores nacionales (españoles).	Computing internacionalmente. • Mercado inmaduro. • Abaratamiento de los costes de infraestructura y mantenimiento tradicionales. • Que se de un sobredimensionamiento de las capacidades del proveedor, que tenga como consecuencia la degeneración de las prestaciones del servicio.

Tabla 3 - DAFO

8.3 Análisis de la elección del modelo en la nube

Este apartado se sustenta en los resultados obtenidos por el análisis DAFO. Después de que la empresa que quiere dar el salto a la nube realice este análisis, dispondrá de la información necesaria para identificar el modelo en la nube que más le conviene.

Como ya sabemos de puntos anteriores de este documento, existen tres tipos de modalidades de servicio en Cloud Computing: SaaS, PaaS e IaaS. De la misma manera sabemos que existen los siguientes tipos de nubes: nubes públicas, privadas, comunitarias e híbridas.

Con los resultados obtenidos en el análisis DAFO y teniendo en cuenta las características y a qué se dedica la empresa que quiere migrar a la nube, se

podrá tomar una decisión de que modelo de servicio, que tipo de nube, etc. nos le beneficia y conviene.

8.4 Análisis de los proveedores Cloud existentes

Después de tomar la decisión de que es viable migrar a la nube, y de qué tipo de nube requiere la entidad y qué modelo de negocio es el apropiado, tenemos que analizar qué proveedores existen con las características que necesita la compañía.

Aunque en apariencia no parezca una tarea como tal, es un paso muy importante, ya que entre la multitud de proveedores que puede haber, las condiciones, legislación, etc. que puedan tener unos u otros pueden ser vitales. Por ello es necesario estudiar cuidadosamente cada una de las opciones que existen en el mercado.

Hoy en día hay multitud de empresas que ofrecen servicios en la nube para los tres tipos de niveles de servicio vistos (SaaS, PaaS e IaaS), al igual que hay gran variedad de proveedores de nubes públicas, privadas e híbridas que ofrecen esos tres niveles de servicio. Hay algunas con gran experiencia en la nube, y otros proveedores que antes ofrecían servicios tradicionales (los que había antes del Cloud Computing) y que ahora han empezado a ofrecer distintos paquetes y servicios en la nube.

Si bien es cierto que las grandes multinacionales del sector como Microsoft, Amazon o Google ofrecen servicios en la nube que pueden ser aplicados a las

necesidades del cliente de forma rápida, en los últimos años ha habido un crecimiento muy importante de proveedores nacionales, como hemos visto algunos ejemplos con anterioridad en este documento, y que deberían ser tenidos en cuenta.

En definitiva, los proveedores cloud nacionales son una gran opción a la hora de realizar este estudio, porque además de tener una serie de características parecidas o diferentes con sus competidores extranjeros, los distribuidores españoles cuentan con la gran ventaja de que cumplen con la legislación de nuestro país, punto que algunos de sus competidores extranjeros no cumple y que en un futuro puede conllevar problemas. Por tanto, no sería una buena opción a la hora de realizar la elección.

8.5 El contrato

Antes de comenzar cualquier relación empresarial siempre tiene que haber un acuerdo legal entre las dos partes, en este caso el proveedor de servicios Cloud Computing y el cliente o contratante de los servicios. Este acuerdo legal es el contrato, el cual regula la relación que establecen ambos, define de forma clara la posición de cada una de las partes, así como las responsabilidades y obligaciones de ambos.

En todo acuerdo comercial los contratos siempre se negocian, pero en el caso del Cloud Computing las cosas son diferentes. Es cada proveedor de servicios en la nube el que facilita a los clientes todas las condiciones en que los servicios son ofrecidos, y es ahí donde el cliente tiene que estudiar con cautela esas condiciones de cada uno de los proveedores cloud que existen para ver cuál de

ellos satisface mejor sus necesidades. Este es otro de los puntos por los que en el apartado anterior se ha hecho énfasis en que el estudio de los distintos distribuidores de servicios en la nube ha de realizarse con sumo cuidado.

Una parte muy importante de un contrato son los términos de uso, los cuales son los encargados de definir las especificaciones técnicas relacionadas con la entrega y la calidad del servicio (en este caso el servicio que el cliente contrata al proveedor cloud). En los términos de uso también se detallan los niveles de rendimiento y disponibilidad que el proveedor garantiza.

Teniendo esto claro, vamos a ver las partes más importantes en las que el cliente tiene que fijarse con atención a la hora de firmar un contrato con un proveedor Cloud Computing:

- Acuerdo de nivel de servicio (ANS), con informes periódicos para que el cliente esté al día de posibles modificaciones, actualizaciones, etc.

- Confidencialidad: Es un aspecto vital ya que los datos, procesos e información del cliente se ejecutarán y almacenarán en la nube.

- Disponibilidad: Este punto es el que se detalla en los términos de uso comentado anteriormente. Define el nivel de disponibilidad que el proveedor de servicios se compromete a cumplir. Lo normal es que todos los distribuidores cloud tengan un nivel de disponibilidad cercano al 100%.

- Pagos: En este punto se especifica lo que el cliente ha de abonar al suministrador cloud por la prestación de los servicios contratados. Ha de

especificarse la cantidad a pagar y la periodicidad en que se deben realizar los pagos.

- Privacidad y cumplimiento normativo: Se trata de una cláusula en la que se definen los niveles de compromiso que el proveedor tiene con el cumplimiento de las leyes de su territorio. También se especifica en qué medida se ajusta a las normas vigentes en territorio español o europeo, sobre todo en cuanto a la privacidad y la protección de los datos (en caso de ser un proveedor que no pertenezca a esta ubicación geográfica).

- Rendimiento: Al igual que la disponibilidad, el rendimiento se define en los términos de uso. Detalla los aspectos que el proveedor garantiza, tales como el ancho de banda, la potencia de cálculo, el nivel de recursos o el almacenamiento.

- Seguridad: En este apartado es donde el proveedor asegura su compromiso de mantener un nivel de seguridad en las instalaciones para mantener sus datos, procesos y equipos. Por ello, debe facilitar al cliente una lista de las medidas de seguridad que aplica en sus sistemas. Es un punto en el que el contratante ha de prestar especial atención, ya que es en este punto en el que han de estar las políticas de gestión de copias de seguridad y respaldo así como la gestión frente a accidentes. Cabe mencionar que es muy recomendable que el proveedor de servicios cuente con un plan de contingencia y recuperación del negocio para poder hacer frente a posibles desastres. El no contar con este plan puede tener como consecuencia que muchos clientes dejen de valorar a ese proveedor como una posibilidad.

- Servicios de soporte: Este apartado se refiere a las obligaciones que el suministrador de servicios se compromete a cumplir en cuanto al soporte prestado al cliente. Uno de los puntos más importantes es el tiempo que necesita el proveedor para recuperarse de un error, por lo que ha de venir especificado.

- Terminación y modificación: Una de las principales características de la computación en la nube es la posibilidad a la hora de modificar los servicios o recursos que se necesitan en cada momento, pudiendo aumentarlos o disminuirlos. Por ello, estas modificaciones han de estar incluidas en el contrato, para evitar posibles malentendidos. Además, el contrato también ha de contener las opciones que el cliente tiene para terminar la relación contractual con dicho proveedor, sobre todo en lo concerniente al borrado y recuperación de la información.

8.6 Cómo realizar la migración a la nube

Una vez realizados todos los pasos anteriores, y después de elegir el proveedor de servicios que mejores condiciones y oportunidades da a la empresa, el último paso que queda es realizar el proceso de migración de los sistemas elegidos a la nube.

Para llevar a cabo este proceso, lo primero que se recomienda es realizar un estudio de todas las posibles consecuencias que puede tener el traspasar todo al distribuidor cloud. Además, se debe asegurar que los datos y la información más crítica de la compañía pasen unos controles muy estrictos y tengan una alta

seguridad, para evitar que la integridad y privacidad de esa información más sensible se vea violada.

En realidad, cada proveedor Cloud Computing tiene su propio sistema de migración, por lo que la propia entidad que decide dar el salto a la nube deberá decidir qué migrar en primer lugar y qué partes dejar para más adelante, es decir, que es recomendable dividir en varias fases la migración.

El dividir en varias fases este proceso tiene una sencilla explicación: Si en la primera fase algo falla o no va bien, se tendrá el resto de partes del sistema aún en el modelo tradicional, por lo que la organización podrá seguir desarrollando su actividad. Por ello, lo primero que se puede migrar son las aplicaciones más pesadas o que más ocupen, dejando los datos, información y procesos críticos para la compañía para fases posteriores (por lo explicado anteriormente). Por ejemplo, como primera etapa se podría pasar el correo a la nube con su servidor correspondiente, y manteniendo el servidor original de datos en local (por si algo va mal, poder volver a lo que se tenía antes y poder continuar con el negocio).

Si la primera fase va bien, ya se podría pensar en migrar la totalidad de aplicaciones, procesos e información a la nube, siempre con los mecanismos que el proveedor que hemos elegido nos facilite. Estos mecanismos con los que cuenta cada distribuidor cloud ayudan a sus clientes a que esta tarea no sea tan compleja como podría ser en un principio. Por ejemplo, algunos proveedores facilitan una interfaz para realizar la configuración del nuevo sistema, mientras que en otros proveedores basta con enviar un email a una dirección que te facilitan donde se han de especificar todos los servicios y datos que se desean migrar a la nube.

Uno de los aspectos más importantes a la hora de realizar la migración a un proveedor de Cloud Computing es mantener una copia de seguridad de todo el sistema tradicional (el que se tenía antes de pasarse a la nube) durante un periodo suficiente de tiempo. Es un aspecto tan importante porque si después de dar el salto a la nube hay algún tipo de problema, en algún momento hay algún fallo, u ocurre un problema imprevisto, siempre podremos volver al modelo que se tenía anteriormente sin que la actividad de la empresa se vea afectada. Además, otra ventaja de realizar esta copia íntegra del sistema tradicional es que se puede ir realizando una integración de las aplicaciones y procesos en el nuevo modelo en la nube de forma transparente para los usuarios.

En el caso de que no se tenga una copia de seguridad de todo el sistema antes de la migración, y si ocurre algún tipo de problema, esto podría tener como consecuencia pérdidas importantes de imagen y/o económicas para la empresa, incluso pudiendo llegar a la finalización de la actividad del negocio de la entidad.

Capítulo 9:

Planificación y presupuesto

9.Planificación y presupuesto

9.1 Planificación inicial

La duración planificada inicialmente para realizar el proyecto fin de carrera fue de 154 días. La planificación se realizó para poder presentar a principios del mes de Septiembre de 2012.

A continuación se detalla el Gantt planificado inicialmente:

Task Name	Duración	Comienzo	Fin
Inicio del proyecto	0 días	mié 28/03/12	mié 28/03/12
FASE DE DELECCIÓN DEL TEMA DEL PFC	**12 días**	**mié 28/03/12**	**jue 12/04/12**
Reunión con el tutor para ver temas disponibles	2 días	mié 28/03/12	jue 29/03/12
Estudio de los temas disponibles para el PFC	6 días	vie 30/03/12	vie 06/04/12
Elección del tema del PFC	2 días	lun 09/04/12	mar 10/04/12
Reunión con el tutor para comunicarle la elección del tema	2 días	mié 11/04/12	jue 12/04/12
FASE DE RECOPILACIÓN Y ESTUDIO DE LA DOCUMENTACIÓN	**32 días**	**vie 13/04/12**	**lun 28/05/12**
Recopilación y estudio de la documentación	25 días	vie 13/04/12	jue 17/05/12
Selección de la documentación adecuada	7 días	vie 18/05/12	lun 28/05/12
FASE DE DESARROLLO DEL PFC	**61 días**	**mar 29/05/12**	**mar 21/08/12**
Desarrollo de los diferentes puntos del PFC	40 días	mar 29/05/12	lun 23/07/12
Entrega del borrador al tutor	2 días	mar 24/07/12	mié 25/07/12
Feedback del tutor	4 días	jue 26/07/12	mar 31/07/12
Modificación del borrador con anotaciones y consejos del tutor	15 días	mié 01/08/12	mar 21/08/12
FASE ENTREGA DEL PFC	**5 días**	**mié 22/08/12**	**mar 28/08/12**
Preparación de la presentación del PFC	3 días	mié 22/08/12	vie 24/08/12
Entrega del PFC	2 días	lun 27/08/12	mar 28/08/12
Hito Fin de proyecto	0 días	mar 28/08/12	mar 28/08/12

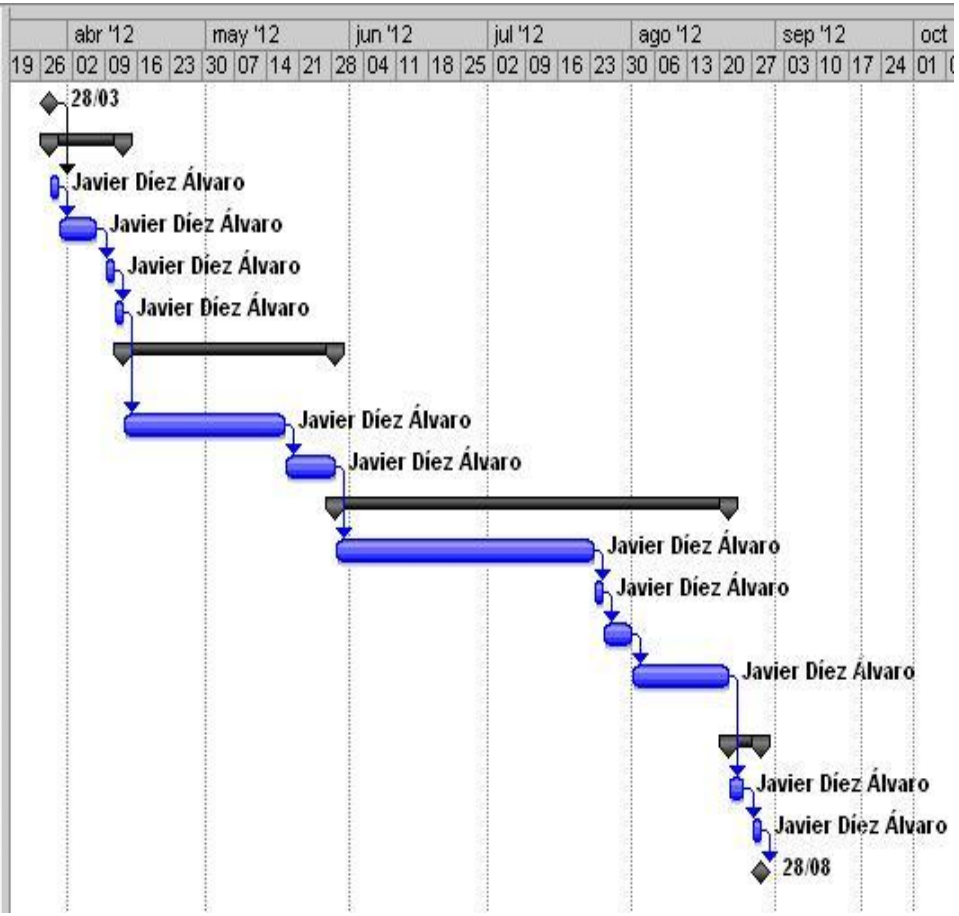

Ilustración 23 - Planificación inicial

9.2 Planificación final

La duración final del proyecto ha sido de 182 días.

El retraso con respecto a lo planificado al principio del proyecto fin de carrera se debe a que durante la primera mitad de año estuve trabajando de becario en una empresa y me quitaba tiempo para poder dedicárselo al proyecto. Otro de los motivos fue que algunas tareas me llevaron algo más de tiempo, como las tareas de *Recopilación y estudio de la documentación* y *Desarrollo de los diferentes puntos del PFC*. El último motivo por el que se ha producido este retraso con respecto a lo planificado inicialmente es que la primera quincena de julio estuve de vacaciones.

En la siguiente ilustración se muestra el Gantt real del proyecto fin de carrera:

Task Name	Duración	Comienzo	Fin
Inicio del proyecto	0 días	mié 28/03/12	mié 28/03/12
FASE DE SELECCIÓN DEL TEMA DEL PFC	**11 días**	**mié 28/03/12**	**mié 11/04/12**
Reunión con el tutor para ver temas disponibles	2 días	mié 28/03/12	jue 29/03/12
Estudio de los temas disponibles para el PFC	6 días	vie 30/03/12	vie 06/04/12
Elección del tema del PFC	2 días	lun 09/04/12	mar 10/04/12
Reunión con el tutor para comunicarle la elección del tema	1 día	mié 11/04/12	mié 11/04/12
FASE DE RECOPILACIÓN Y ESTUDIO DE LA DOCUMENTACIÓN	**36 días**	**jue 12/04/12**	**jue 31/05/12**
Recopilación y estudio de la documentación	29 días	jue 12/04/12	mar 22/05/12
Selección de la documentación adecuada	7 días	mié 23/05/12	jue 31/05/12
FASE DE DESARROLLO DEL PFC	**67 días**	**vie 01/06/12**	**mar 18/09/12**
Desarrollo de los diferentes puntos del PFC	46 días	vie 01/06/12	lun 20/08/12
Entrega del borrador al tutor	2 días	mar 21/08/12	mié 22/08/12
Feedback del tutor	2 días	jue 23/08/12	vie 24/08/12
Modificación del borrador con anotaciones y consejos del tutor	17 días	lun 27/08/12	mar 18/09/12
FASE ENTREGA DEL PFC	**5 días**	**mié 19/09/12**	**mar 25/09/12**
Preparación de la presentación del PFC	3 días	mié 19/09/12	vie 21/09/12
Entrega del PFC	2 días	lun 24/09/12	mar 25/09/12
Hito Fin de proyecto	0 días	mar 25/09/12	mar 25/09/12

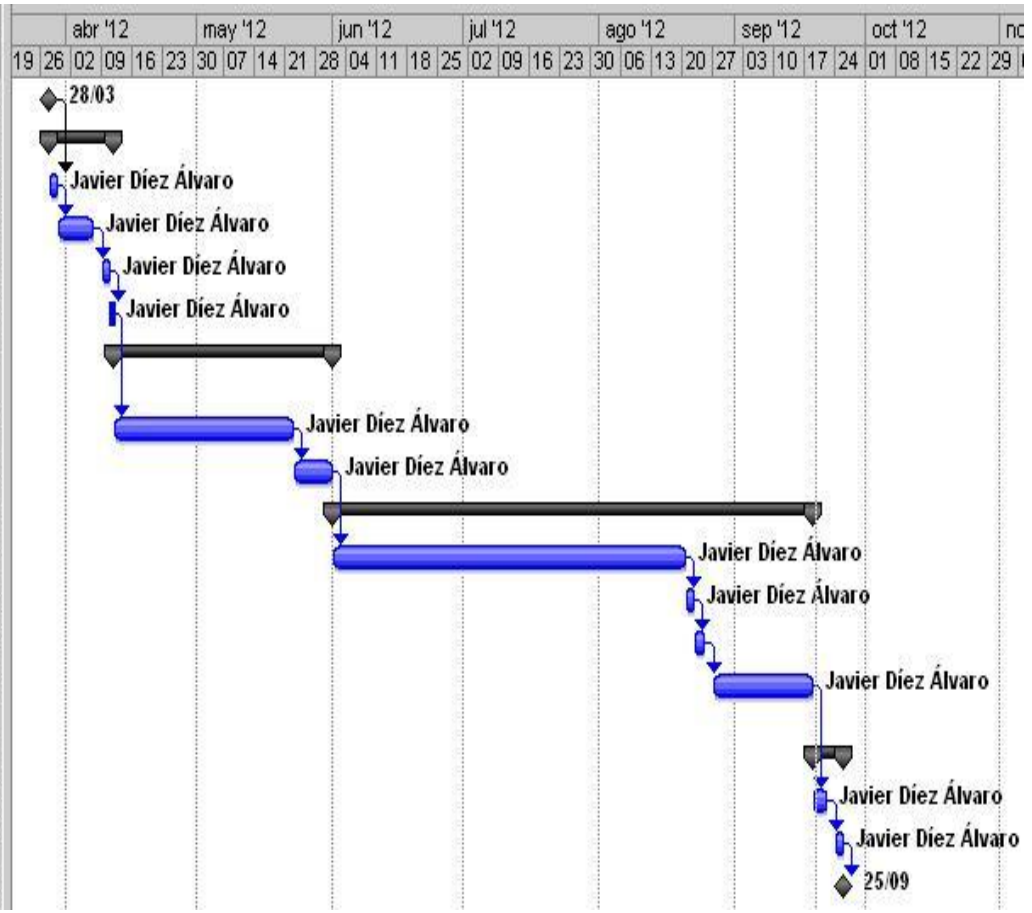

Ilustración 24 - Planificación final

9.3 Presupuesto

El presupuesto final del proyecto es el que se desglosa en las tablas siguientes:

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor:
Javier Díez Álvaro
2.- Departamento:
Informática
3.- Descripción del Proyecto:

- Titulo	Los entornos en nube (Cloud Computing): …
- Duración (meses)	6
Tasa de costes Indirectos:	20%

4.- Presupuesto total del Proyecto (valores en Euros):
Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a titulo informativo)	Categoría	Dedicación (hombres mes) a)	Coste hombre mes	Coste (Euro)
Javier Díez		Ingeniero Técnico	6	651,00	3.906,00
			Hombres mes 6	**Total**	3.906,00

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable d)
Ordenador	480,00	100	6	24	120,00
Licencia Microsoft Office	350,00	100	6	24	87,50
				Total	207,50

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
	Total	0,00

OTROS COSTES DIRECTOS DEL PROYECTO e)

Descripción	Empresa	Costes imputable
Material de oficina		120,00
	Total	120,00

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	3.906
Amortización	208
Subcontratación de tareas	0
Costes de funcionamiento	120
Costes Indirectos	847
Total	5.080

Tabla 4 - Presupuesto

Capítulo 10:

Conclusiones

10. Conclusiones

Las conclusiones que saco una vez finalizado el proyecto fin de carrera son muy positivas. Para empezar, los objetivos que me fijé al comienzo del proyecto se han cumplido. Al principio veía este proyecto como algo complejo ya que no sabía de dónde iba a poder sacar la información suficiente y fidedigna para poder documentar como es debido este proyecto. Pero después de todos estos meses me doy cuenta de que he adquirido grandes conocimientos acerca de este nuevo modelo que trata el proyecto, el Cloud Computing. Por esta razón recomiendo a toda persona que sienta curiosidad, interés o necesidad por saber de este tema, que lea este documento.

Se han cumplido los objetivos marcados al comienzo de este documento, que consideré que eran los puntos más importantes a tratar a la hora de hablar de este tema:

- Se ha definido de forma clara qué son los entornos en la nube, se ha hablado de la historia que tiene este modelo a pesar de ser un sistema muy joven, y de las razones de su nacimiento.

- Se han clasificado los cuatro tipos de nubes que existen y los tres niveles de servicio que existen en el Cloud Computing, con sus características y propiedades.

- Se ha aclarado qué papel tiene la virtualización en los entornos en nube, así como sus características y algunos ejemplos que existen hoy en día.

- Se ha realizado un amplio abanico de ejemplos de sistemas Cloud existentes en la actualidad según el servicio que ofrezcan (SaaS, PaaS o

IaaS). Además, se ha enfatizado en las empresas y proveedores que ofrecen servicios en el territorio Español.

- Se ha conseguido aclarar cuál es la legislación aplicable al Cloud Computing, ya que no hay un marco que regule los entornos en la nube como tal (ni en España ni a nivel internacional). Solo hay aspectos, leyes y puntos que se pueden ir aplicando, desde la regulación de la LOPD, de la LSSI y del Código penal. Además, se proponen vías de implantación de algunas de algunas de las leyes incluidas en el RDLOPD.
  Teniendo en cuenta el nivel de crecimiento que está teniendo el Cloud Computing en estos últimos años, es probable que de aquí a unos años haya un marco que regule específicamente este sistema.

- Asimismo, se han clasificado los principales riesgos que conlleva la utilización de servicios alojados en la nube.

- Se ha realizado una guía con los pasos que se han de dar cuando una empresa o un usuario quiera dar el salto a la nube, las decisiones que tiene que ir tomando, etc.

En definitiva, se han cumplido los objetivos marcados al comienzo del proyecto, con lo que he ganado grandes conocimientos sobre este modelo que está en constante crecimiento y desarrollo.

Capítulo 11:

Referencias y bibliografía

11. Referencias y bibliografía

11.1 Referencias

[1] TICbeat, http://cloud.ticbeat.com/8-10-empresas-emplean-nube/

[2] TICbeat 2, http://cloud.ticbeat.com/6-cada-10-empresas-espanolas-nube/

[3] Routing the Word, http://routingtheworld.wordpress.com/spanish-content/nube-publica-nube-privada-nube-hibrida-y-nube-super-hibrida/

[4] Cloud Computing: What It Is -- Along With the Pros & Cons, http://blog.nskinc.com/IT-Services-Boston/bid/84614/Cloud-Computing-What-It-Is-Along-With-the-Pros-Cons

[5] Continuidad en su negocio, http://nunsys.com/continuidad-en-su-negocio/

[6] Virtualización, http://sliceoflinux.com/virtualizacion/

[7] NetPC Virtualización, http://prcticasderedes.blogspot.com.es/2012/04/virtualizacion-la-virtualizacion.html

[8] Thomasmaurer, http://www.thomasmaurer.ch/2011/04/windows-server-2008-r2-hyper-v-licensing-overview/

[9] Donde el futuro es el presente, http://enteratedelfuturo.wordpress.com/2012/05/30/un-hacker-hace-publico-codigo-de-vmware/

[10] syncron, http://www.syncron.be/component/content/article/54-banner/98-xen-server-backup.html

[11] Nixmint, http://nixmint.blog.tut.by/2012/09/08/virtualbox-4-1-20-for-linux/

[12] The harvest blog, http://www.getharvest.com/blog/2010/10/akacrm-announces-harvest-for-salesforce-application/

[13] Google Apps en el ámbito universitario, http://blog.catedratelefonica.deusto.es/google-apps-en-el-ambito-universitario/

[14] Google Apps, http://www.google.com/apps/intl/es/index.html

[15] Apple, http://www.apple.com/la/icloud/

[16] Aprendo gratis el blog, http://blog.aprendogratis.com/tag/office-365/

[17] Zoho, http://www.zoho.com/logos.html

[18] Google App Engine Java Experiments, http://freecomputerbooks.com/Google App-Engine-Java-Experiments.html

[19] Force.com & Heroku, http://www.salesforce.com/es/platform/?d=70130000000FJqO&internal=true

[20] Cloud innovation, http://www.cloudinnovation.be/en/force-dot-com/

[21] Facebook app development using Heroku, http://www.dkartheek.com/2011/09/facebook-app-development-using-heroku.html

[22] Meet Windows Azure Event, http://www.phpbenelux.eu/en/meet-windows-azure

[23] AWS introduces CloudSearch, http://www.latestdigitals.com/2012/04/12/aws-introduces-cloudsearch/

[24] CloudKick, https://www.cloudkick.com/providers/gogrid/

- DosControl en la nube, http://www.doscontrol.com/cloud-computing/tipos-de-nubes

- Blog BCN Binary. Tecnología e Informática http://bcnbinaryblog.com/los-distintos-tipos-de-cloud-computing-%C2%BFcual-le-conviene-a-mi-empresa/

- Societic, http://www.societic.com/2010/06/cloud-computing-tipos-de-nubes-de-aplicaciones/
- Computación en nube, http://www.computacionennube.org/13/tipos-de-nube/
- Nubes públicas, privadas e híbridas, http://www.itnews.ec/marco/000036.aspx
- Sociedad conectada, voz y voto, http://vozyvoto.es/2010/07/01/cloud-computing/
- Alegsa, http://www.alegsa.com.ar/Dic/virtualizacion.php
- Virtualización y computación en la nube, http://www.mercadeo.com/84_virtualizacion.htm
- Ventajas de la virtualización, http://www.itnews.ec/marco/000171.aspx
- Blog tecnológico y administrativo, http://makenard.blogspot.com.es/2009/08/virtualbox-mas-que-un-programa-una.html
- Pensando en sistemas de virtualización, http://blog.abserver.es/pensando-en-sistemas-de-virtualizacion%E2%80%A6/
- Windows Azure, http://www.windowsazure.com/es-es/
- Introducción a Windows Azure, http://es.scribd.com/doc/78204537/Subete-a-La-Nube-de-Microsoft-Parte-1-Introduccion-a-Windows-Azure
- Salesforce, http://www.salesforce.com/es http://www.salesforce.com/es/platform/products.jsp
- Programación en la nube, http://www.genbetadev.com/programacion-en-la-nube/introduccion-a-google-app-engine

- Google developers, https://developers.google.com/appengine/docs/whatisgoogleappengine?hl=es https://developers.google.com/appengine/casestudies?hl=es#3scale

- Blogsdna, http://www.blogsdna.com/1232/top-10-best-web-application-hosted-on-google-app-engine.htm

- Thetechtrendz, http://blog.thetechtrendz.com/2010/07/top-10-best-google-app-engine-apps.html

- SaaSandgo, http://www.saasandgo.com/

- DosControl, http://www.doscontrol.com/soluciones/blog

- Gogrid, http://www.gogrid.com/

- Amazon Web Services, http://aws.amazon.com/es/products/

- Bcnbinary, http://www.bcnbinary.com/es/Soluciones/1/Cloud_Computing/

- Los 8 riesgos más grandes del Cloud Computing, www.marketingdirecto.com/actualidad/tendencias/los-8-riesgos-mas-grandes-del-cloud-computing/

- Bases de datos de legislación, http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t10.html#a197

- BOE, http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf http://www.boe.es/boe/dias/2010/06/23/pdfs/BOE-A-2010-9953.pdf http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

- Ley de Servicios de la Sociedad de la Información, http://www.minetur.gob.es/telecomunicaciones/lssi/paginas/index.aspx www.minetur.gob.es/telecomunicaciones/lssi/Documents/ltriptico.pdf

- Agencia Española de Protección de Datos, https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php http://www.agpd.es/portalwebAGPD/canalciudadano/preguntasciudadano/transferencias_internacionales/index-ides-idphp.php

- Diario oficial de la Unión Europea, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:227:0011:0014:ES:PDF

- Saasmania, http://www.saasmania.com/blog/2008/09/18/un-dafo-para-el-cloud-computing/

11.2 Bibliografía

- Documento Sun-Cloud-Computing.pdf.

- Suplemento del nº114 de la revista Channel Partner, de Septiembre 2011.

- Suplemento del nº117 de la revista Channel Partner, de Diciembre 2011.

- Revista Channel Partner nº120 Marzo 2012.

- Suplemento del nº123 de la revista Channel Partner, de Junio 2012.

- Guía para empresas: seguridad y privacidad el Cloud Computing, por Inteco.

- Estudio sobre el Cloud Computing en el sector público en España, por Inteco.

- Riesgos y amenazas en Cloud Computing, por Inteco-Cert.

- Apuntes de Auditoría Informática, de la Universidad Carlos III de Madrid.

- Apuntes de Gestión de proyectos, de la Universidad Carlos III de Madrid.